PAULO MURILO SILVA

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES

FLORIANÓPOLIS - SC

2003

UNIVERSIDADE FEDERAL DE SANTA CATARINA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

PAULO MURILO SILVA

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação

Profº Dr Luiz Fernando Jacintho Maia

Professor Orientador

Florianópolis, novembro de 2003.

POLÍTCA DE SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES

Paulo Murilo Silva

Esta dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação Área de Concentração de Sistema de Conhecimento e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

_____
Fernando Álvaro Ostuni Gauthier, Dr

Banca Examinadora

_____
Luiz Fernando Jacintho Maia, Dr. (Orientador)

_____
José Mazzucco Junior, Dr.

_____
João Bosco da Mota Alves, Dr.

SUMÁRIO

LISTA DE FIGURAS E TABELAS

RESUMO

O presente estudo trata das técnicas de elaboração de uma política de segurança da informação adotada por organizações de combate a invasão de rede de computadores. Dada a importância da segurança em ambientes computacionais, este assunto relatará o trabalho de alguns grupos de trabalho que testam técnicas de invasão, relatam invasões ocorridas em empresas e universidades, avaliam softwares e ferramentas para serem aplicadas na tentativa de diminuir as possibilidades de uma invasão.

Apresentaremos aqui as orientações de organismos como o Computer Emergency Response Team (CERT), da Universidade Carnegie Mellon, e o System Administration, Networking and Security Institute (SANS), organização americana de cooperação, pesquisa e educação, e também de organizações brasileiras como o NIC BR Security Office (NBSO), o Centro de Atendimento a Incidentes de Segurança (CAIS-RNP) e a Equipe de Segurança da Universidade Estadual de Campinas-UNICAMP.

Serão vistas algumas ferramentas de prevenção e de ataques hackers, disseminação de vírus e falhas/bugs em softwares de computadores, bem como o estudo de caso da Universidade Estadual do Oeste do Paraná e proposta de educação aos usuários da universidade.

ABSTRACT

This study is about the techniques of elaboration of a information security policy used by combat companies the computer network invasion. Due to importance of security in computing environments, this topic will relate the work of some working groups which test invasion techniques, relate invasions that occurred in companies and universities, evaluate softwares and tools to be applied in the attempt to diminish the possibilities of an invasion.

We will present here the orientations of organisms such as the Computer Emergency Response Team (CERT), from Carnegie Mellon University, and System Administration, Networking and Security Institute (SANS), American organization of cooperation, researches and education, and also from Brazilian organizations like the NIC BR Security Office (NBSO), the Centro de Atendimento a Incidentes de Segurança (CAIS-RNP) and Security Team from Campinas State University - UNICAMP.

It will also be seen some tools of hackers prevention and attack, virus dissemination and failures/bugs in computers softwares, as well as a Universidade Estadual do Oeste do Paraná - UNIOESTE study case and a education propose for user of university.

1. INTRODUÇÃO

Segurança da informação é a conjunção de uma estratégia e de ferramentas específicas que atendam as necessidades corporativas para a manutenção de um ambiente saudável. Considerada um item vivo, a política de segurança nunca está acabada e deve ser desenvolvida e atualizada durante toda a vida da empresa.

Segurança de rede é um processo dinâmico e o inimigo é humano. Um evento isolado não causa estrago, mas sim a conjunção de processos mal resolvidos. Segundo Roger Davis, diretor sênior da Nu Skin International, "as corporações têm que aprender a reconhecer fatores humanos e políticos, para conseguir gerenciar todas as suas áreas de negócios, afetadas constantemente por pragas virtuais", durante a RSA Conference, em fevereiro de 2002.

Computadores e redes podem mudar nossas vidas para melhor ou pior. A disseminação de redes, e particularmente, da Internet, é o fenômeno tecnológico de maior impacto social atualmente. Até pouco tempo atrás, as organizações implementavam suas redes apenas com o objetivo de prover funcionalidades que permitiam agilizar processos internos. A presença da Internet e a popularização do microcomputador trouxeram um novo ambiente, anárquico, descontrolado com grandes possibilidades, necessitando de um maior controle sobre as informações que circulam por estas máquinas e redes corporativas.

A importância da segurança cresce ainda mais rapidamente, quando se leva em consideração o rápido aumento da complexidade das conexões. A segurança

é inversamente proporcional às funcionalidades. Quanto maiores as funcionalidades, como serviços e aplicativos, menor é a segurança no ambiente.

Isso pode ser explicado pelos seguintes fatores (NAKAMURA e GEUS, 2001):

- Exploração da vulnerabilidade em sistemas operacionais, aplicativos, protocolos e serviços;
- Exploração do aspecto humano das pessoas envolvidas;
- Falha no desenvolvimento e implementação da política de segurança;
- Falha na configuração de serviços e de sistema de segurança;
- Desenvolvimento de ataques mais sofisticados.

As obrigações dos administradores quanto à manutenção da segurança devem estar claramente definidas na política de segurança da organização, como é o caso do acompanhamento das novidades e dos boletins sobre os sistemas que estão sendo utilizados na organização.

A confiabilidade e a disponibilidade das estruturas de redes passam a ser essenciais para o bom andamento das organizações. A segurança de redes significa muito mais que a proteção contra hackers, maus funcionários ou vírus. A segurança de redes significa permitir que as organizações busquem os seus lucros, portanto ela deve ser considerada um elemento habilitador para que o negócio da organização seja realizado.

Esta importância pode ser observada no momento que esta organização abre as portas para o meio digital, o e-commerce, o e-marketing. A estrutura da

Internet que se apresenta para mostrar esta organização para o mundo, não só para a região a que ela está inserida.

Nas décadas de 70 e 80, quando os mainframes dominavam os centros de processamento de dados (CPDs), os aspectos de segurança eram relacionados com o nome do usuário e em sua senha. Naquele tempo a informática fazia parte da retaguarda das organizações, onde o enfoque principal de segurança era a confidencialidade dos dados manipulados. Atualmente, o alto grau de conectividade e a grande competitividade trouxeram outros tipos de problemas e a informática tornou-se essencial nos negócios e as informações devem estar disponíveis para a equipe de trabalho, porém devem estar protegidas.

Um exemplo em que fica claro que a segurança tem uma forte ligação nos negócios é o próprio ambiente cooperativo. O sucesso depende, muitas vezes, da comunicação segura entre matrizes, filiais, fornecedores e clientes.

Porém, a segurança é vista como um elemento supérfluo dentro das organizações, onde os orçamentos são limitados e a segurança acaba ficando em segundo plano, obtendo maior importância quando esta organização sofre algum incidente de segurança.

Com a importância estratégica que a tecnologia de informação vem conquistando, os prejuízos com invasões e incidentes de rede causam, a cada ano, maior impacto nos negócios das organizações. O controle do que acontece nas redes corporativas tem sido um dos pontos mais frágeis das organizações.

1.1. Origem do Trabalho

Com a importância estratégica que a tecnologia de informação vem adquirindo ao longo dos anos, os prejuízos com invasões e incidentes de rede que estão ocorrendo está fazendo com que as organizações dispensem maior atenção com o armazenamento e manipulação de dados de maior impacto aos negócios. O controle do que acontece nas redes corporativas tem sido um dos pontos mais frágeis das organizações.

As organizações não possuem a "cultura da segurança". Quando se fala em segurança do patrimônio, associa-se imediatamente à figura do vigilante, porteiro. Segurança do patrimônio deve ser entendido como sistema de proteção e prevenção que a organização dispõe para resguardar as instalações, equipamentos, tecnologia, pessoal e informação. Devem ser avaliados os riscos a que estão expostas e definir procedimentos adequados de conduta. Esta situação requer o engajamento de todos os colaboradores, porque deve haver um comprometimento de todos para que a segurança seja uma ação de equipe e não um ato isolado. A informação é o ativo mais valioso da organização. Apesar da maioria do corpo executivo estarem conscientes da necessidade da criação e cumprimento de uma política de segurança, faz-se necessário estar sempre lembrando que deve haver um investimento para gerenciar e mantê-las.

Porém, no ano de 2001, a maioria das organizações, a imprensa e os órgãos que controlam o tráfego de dados pela internet e pelas redes

corporativas, colocaram em evidência a necessidade de se ter uma política de segurança para gerenciar a troca de informações entre máquinas ligadas em rede. Novas pragas tecnológicas estão atacando. Novos meios de invasão são descobertos, várias falhas em sistemas operacionais, softwares gerenciadores de dados e softwares de correspondência eletrônica. O ano de 2001 foi extraordinário em danos causados pelas invasões de hackers, vírus e worms, bugs de sistemas, que se disseminaram pela Internet e, conseqüentemente, pelas redes locais de computadores. Houve muito prejuízo financeiro e de perda de informações no mundo todo. Em 2002, não foi diferente, e a cada ano que se seguir estes ataques se intensificarão. No final de 2002 foi registrado o dobro de ocorrências do ano anterior, problemas em programas largamente utilizados e a correria para correções foi frenética. Isto tudo porque as organizações não possuem uma política de segurança definida, ou se possuem não as aplicam ou não as atualizam. É necessário estar atualizado com novas tecnologias de prevenção, atualizações de programas, diagnóstico e soluções para ataques e invasões de sistemas corporativos de rede de computadores, técnicas de recuperação de dados perdidos, políticas claras e definidas para uso de equipamentos de informática dentro das organizações. Usuários esclarecidos quanto aos problemas advindos do acesso a dados não permitidos, e punições definidas para tal intuito.

1.2. Importância do Trabalho

Este trabalho tem por objetivo estudar as políticas de segurança, algumas soluções às ameaças e vulnerabilidades existentes em uma rede corporativa. As políticas de seguranças devem ser revistas e atualizadas sempre. Este é um trabalho que deve ser contínuo em organizações que possuem um volume de dados e informações abertos à consulta através de redes. Assim é preciso ter um controle rígido de acesso aos equipamentos que compõem o sistema de redes. Este controle deve ser grande também através do acesso interno, uma vez que pesquisas revelam que a grande parte de informações retiradas das organizações é feita por pessoas de dentro da própria organização. Políticas de segurança definem o bom andamento da informação dentro da organização, se aplicadas corretamente e em constante atualização.

1.3. Justificativa

Muitas pessoas ao tratarem do assunto segurança, já vinculam a configuração de determinada ferramenta, software ou hardware da topologia de sua rede como uma segurança implantada. Pode-se dizer que não estão totalmente errados, houve um passo em direção à implantação da segurança da informação, mas, para que a segurança seja realmente efetiva, são necessárias

a avaliação e a determinação de medidas de segurança que passem pela tecnologia, pelos processos e pelas pessoas.

Política de segurança é um tema de grande interesse para o controle de acesso às informações armazenadas em redes corporativas.

1.4. Objetivos

1.4.1. Objetivo Geral

Apresentar algumas recomendações de políticas de segurança adotadas e defendidas por organismos de controle de segurança quanto à invasão de redes corporativas e suas características de segurança, limitação de acesso de dados por terceiros, e mecanismos de combate à intrusão interna e externa. Elaborar uma metodologia para a conscientização do usuário final sobre regras básicas de segurança da informação.

1.4.2. Objetivos Específicos

Apresentar as recomendações de políticas de segurança e de prevenção de ataques a redes de computadores, regras básicas para a elaboração de uma política de segurança da informação, através de

mecanismo de restrição de acessos internos e externos da rede, sem inviabilizar o uso das novas tecnologias no desenvolvimento do trabalho diário.

Identificar pontos críticos de falha de segurança por parte dos usuários da Universidade Estadual do Oeste do Paraná quando da elaboração de senhas, manipulação de informações e comunicação através de correio eletrônico. Elaborar uma proposta metodológica para conscientizar e educar os usuários desta universidade sobre regras básicas de segurança de informação e para a implementação de uma política de segurança.

1.5. Limitações do Trabalho

Este trabalho se limitará as políticas de segurança da informação e de redes de computadores e a importância destas políticas para comunidade acadêmica da Reitoria da Universidade Estadual do Oeste do Paraná - UNIOESTE. Não é pretensão deste trabalho elaborar um inventário de todas as técnicas existentes, mas descrever algumas técnicas mais representativas bem como as falhas mais comuns em ataques a computadores, roubo ou perda de informações, e definição de senhas.

1.6. Estrutura do Trabalho

Este trabalho tem seqüência com a fundamentação teórica/revisão literária do assunto em um capítulo distinto. A seguir, em dois capítulos, analisa algumas ameaças, prevenções e proteções aos sistemas computacionais. No capítulo seguinte trata do estudo de caso da Universidade Estadual do Oeste do Paraná , avaliando o conhecimento dos usuários na manipulação das informações pertinentes à instituição e elaboração de uma proposta de educação ao usuário. No capítulo seguinte são feitas as conclusões e recomendações de trabalhos futuros, finalizando com referencial teórico consultado.

2. POLÍTICA DE SEGURANÇA

2.1. Rede de Computadores

A RFC-2828 (Request for Coments nº 2828) define rede de computadores como uma coleção de hosts interligados para a troca de dados. Na mesma rfc é definido host como sendo um computador ligado a uma rede de comunicação que possa usar os serviços providos pela rede para trocar dados.

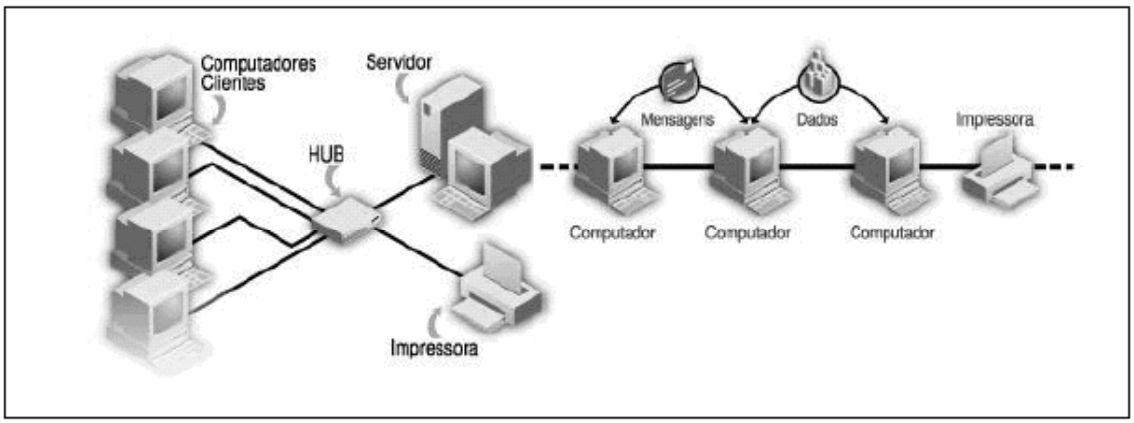

Figura 2.1: Exemplo de uma rede de computadores. Fonte: www.timaster.com.br

Para Tanenbaum (TANENBAUM, 1994), o termo “rede de computadores” pode ser definido como um conjunto de computadores autônomos, interconectados, sendo capazes de trocar informações. Essa interconexão pode ser feita através de fios de cobre, lasers, microondas, satélites de comunicações e também por fibras óticas.

2.2. Política de Segurança

É definida pela RFC-2828 como sendo o conjunto de regras e práticas que especificam ou regulam, como um sistema ou organização provê serviços seguros, protegendo os recursos críticos do sistema.

A evolução das redes de computadores identificou um importante equipamento de gerenciamento que é o servidor de redes. Sua função principal é prover serviço de comunicação, acesso e validação de usuários. Também é comum armazenarem dados valiosos para a organização. Não raro um único servidor de rede centraliza todos os dados da empresa, e ainda fornece acesso às outras máquinas a ele conectadas, faz papel de saída para acesso à rede mundial de computadores, a Internet.

Se houver alguma brecha no acesso a este equipamento, teremos uma situação crítica aqui, e provavelmente haverá perda de dados armazenados neste equipamento.

Também em estações de trabalho é comum existirem informações armazenadas sem maiores cuidados em protegê-las de um acesso externo, ou mesmo por pessoas de dentro da organização, porém sem acesso a tais informações.

Redes de computadores tornaram-se indispensáveis na condução de negócios, tomadas de decisão, em governos, em meios acadêmicos, etc. Sistemas interligados possibilitam acesso à informação rapidamente, reduzem custos e tempo de deslocamento entre unidades. Pode haver também

comunicação através da Internet, que possibilita uma gama maior de serviços, e também do comércio eletrônico.

Todas estas possibilidades e outras não citadas aqui se tornaram possíveis graças aos sistemas de redes de computadores. Porém, além das vantagens, surgiram os riscos de acessos não autorizados aos dados da organização. Questionamentos do tipo, meus dados estão protegidos? Alguém pode acessar minha máquina? Quem está vulnerável a estes acontecimentos?

As respostas para estas perguntas são: todos estão vulneráveis, sim seus dados podem ser acessados por terceiros. Todos que possuem uma infra-estrutura de tecnologia de informação montada e funcionando em rede distribuída pode sofrer ataques e precisa necessariamente ter uma política de segurança definida, atuante e atualizada.

Técnicas de contra-medidas de invasão tornam-se ineficazes muito rapidamente. Novas técnicas de invasão são descobertas diariamente, tornando-se impossível manter redes de computadores 100% seguras.

A habilidade em configurar e operar seguramente sistemas não necessariamente significa que estes sistemas estarão seguros amanhã. Experientes invasores estão ficando mais sofisticados em seus ataques, enquanto novatos estão aprendendo com receitas colocadas a disposição na Internet e utilizam sem precisar de maiores conhecimentos. Porém estes são descobertos e anulados mais rapidamente e suas técnicas de ataque já são bem conhecidas pelos administradores de redes.

Dois dos grandes vilões dos administradores de redes e suas informações são a Negação de Serviços (DoS) e a disseminação de vírus e worms. Tipos de problemas que estão aumentando em escala geométrica.

Muitos problemas de segurança poderiam ser evitados se os administradores de rede configurassem corretamente os computadores e mantivessem estas configurações atualizadas (ALLEN, 2000). Algumas medidas podem ser tomadas para uma segurança mais efetiva, como por exemplo, a instalação e configuração de somente o essencial no sistema operacional, não aceitando a instalação default e sem as perfumarias que não são necessárias para o bom funcionamento dos equipamentos e das redes, ou então a instalação de patches de correção, atualização de programas, controle de privilégios de acesso. Estas são algumas das recomendações mais corriqueiras dadas pelas instituições que monitoram ataques a redes. Outro procedimento é a divulgação ou a comunicação de que a empresa sofreu um ataque e qual a conseqüência deste ataque. Assim os organismos responsáveis pelo monitoramento estão sempre atualizados com as informações de procedimentos a serem tomados.

O estudo das ameaças é fundamental para elaborar uma política de segurança adequada. Saber quem se interessa por suas informações é o objetivo principal para proteger sua organização.

Existem os ataques que não visam o roubo da informação, mas sim a satisfação de contar aos amigos que invadiu tal empresa, ou o ataque de destruição dos dados por vírus, o mais comum.

Há também os ataques que visam o roubo de informação, conhecido como espionagem industrial e/ou comercial, que já envolvem uma esfera judicial em

países como Estados Unidos e Inglaterra, onde já existe jurisprudência para estes casos. Estes ataques trazem grandes prejuízos as organizações.

Não existem sistemas totalmente seguros, como foi mencionado anteriormente, porém uma boa alternativa é avaliar a motivação, a habilidade e a oportunidade que o atacante possuí. Deve-se definir o que proteger, priorizar regras e normas para ataques internos ou externos. Enaltecer a frustração do ataque, tanto por pessoas como por vírus. Definir o nível aceitável de risco que poderá ter a rede da organização. Aplicar o que está definido na política de segurança quanto a punições. Mesmo não estando conectados à Internet, existe a possibilidade de invasões internas e os responsáveis por estes ataques devem ser punidos conforme as normas estabelecidas.

Segurança não é uma tecnologia, é um processo de administração a níveis aceitáveis de risco (WADLOW, 2000). Este processo de administração é composto por análise, síntese e avaliação.

Políticas de Segurança definem regras que regulamentam como a organização gerenciará e protegerá suas informações. As políticas e os procedimentos de contra-medidas devem ser documentados e conhecidos pelos administradores e usuários dos recursos computacionais. A alta direção deve ser engajada a aderir a primeira hora as políticas recomendadas. Os usuários devem ser consultados se as políticas elaboradas não irão afetar de maneira radical o desenvolvimento de seus trabalhos, chegando a atrapalhar o bom desempenho dos trabalhos. Todos devem tomar conhecimento e respeitar as normas das políticas de segurança, que devem ser sempre atualizadas, juntamente com os procedimentos de contra-medidas.

Uma política de segurança é um documento difícil de ser escrito. Não é um documento permanente, deve ser constantemente atualizado. Deve descrever o que está protegendo.

A política de segurança da informação deve seguir quatro paradigmas básicos em sua composição (JASONBS, 2002):

- Integridade: a condição na qual a informação ou os recursos da informação é protegido contra modificações não autorizadas;
- Confidencialidade: propriedade de certas informações que não podem ser disponibilizadas ou divulgadas sem autorização prévia do seu dono;
- Disponibilidade: característica da informação que se relaciona diretamente à possibilidade de acesso por parte daqueles que a necessitam para o desempenho de suas atividades;
- Legalidade: estado legal da informação, em conformidade com os preceitos da legislação em vigor.

As principais ameaças a serem tratadas pela política de segurança não condizem somente com o acesso não autorizado, mas também com as estruturas físicas do ambiente e podem ser elencadas como (JASONBS, 2002):

- Integridade;
- Ameaças de ambiente (fogo, enchente, catástrofes,...);
- Erros humanos;
- Erros de hardware;
- Falhas de sistema
- Fraudes;

- Divulgação e manipulação de informações não autorizadas; entre outros.

O componente mais importante de uma estratégia geral de segurança é ter uma política de segurança robusta. Uma política de segurança define o que se considera aceitável em termos de segurança e o que será feito no caso de se detectar violações do que for estabelecido. (CERT-RS, 2000).

Em termos gerais, políticas são diretivas de gerenciamento que estabelecem metas comercias da organização, fornecem uma estrutura de implementação para alcançar objetivos dessas metas e atribuem responsabilidades e domínios ao processo. Devem incluir regras detalhadas definindo como as informações e recursos da organização devem ser manipulados, o que é, e o que não é permitido em termos de segurança, durante a operação de um dado sistema. (BERNSTEIN et al. 1997).

A política de segurança deve prover gerenciamento dos riscos que a empresa incorre ao buscar objetivos comerciais.

O primeiro passo a ser tomado na implantação de uma política de segurança é definir as metas, conferindo quais restrições impor. Para uma política de segurança sólida, é essencial a avaliação de determinados critérios como: (CERT-RS, 2000; ANÔNIMO, 2000):

- Flexibilidade: a medida em que a empresa evoluir, é preciso rever e atualizar esta política de modo a refletir as novas aplicações e tecnologias bem como as novas comunidades de usuários;
- Pertinência: reflexão dos objetivos comerciais da empresa;

- Aplicabilidade: elaboração deve estar baseada nas realidades do ambiente computacional;
- Atualidade: a política deve estar sempre sofrendo atualizações, brechas são descobertas constantemente;
- Facilidade de uso: o sistema mais fácil de usar permitiria acesso a qualquer usuário e não requereria senha, isso quer dizer, não haveria nenhuma segurança. Requerer senhas torna o sistema um pouco menos conveniente, mas mais seguro;
- Custo/Benefício: existem diversos custos para implantação de segurança: o monetário (custo de comprar hardware de segurança e software como firewalls e geradores de senhas descartáveis); desempenho (cifragem de dados consome tempo); e facilidade de uso. Porém há diversos riscos: perda de privacidade (a leitura de informação por indivíduos sem autorização), perda de dados (a corrupção ou deleção de informação) e a perda de serviço (por exemplo, o preenchimento do espaço de armazenamento de dados, uso de recursos computacionais, e negação de acesso à rede). Devendo ser importante a avaliação do custo contra cada tipo de perda;
- Integração: a política de segurança na Internet deve ser bem integrada com a política geral de proteção aos sistemas de informação;
- Serviços oferecidos: cada serviço oferecido apresenta um próprio risco de segurança, o administrador deve avaliar e decidir se o risco

que o mesmo apresenta excede em valor o benefício do serviço, desabilitando ou mantendo ativo.

A política de segurança também significa delegar responsabilidades para os colaboradores que passam a responder por seus atos. A importância da conscientização da equipe profissional da organização é consenso entre especialistas de segurança (BARBOSA, 2001).

2.3. Políticas de Controle de Acesso

A política de segurança estabelecida deve se preocupar também com o controle de acesso de pessoas a ambientes da organização. Controlar acesso físico por parte de staff designado para isto. Em instituições públicas de ensino, por exemplo, este controle é quase inexistente, apenas poucas pessoas controlam grandes áreas de prédios e o acesso pode ser facilitado pelo grande fluxo por corredores e salas.

O escopo da política adotada deve compreender as instalações físicas da empresa e também a lógica. Tanto acessos físicos como virtuais devem ser monitorados e controlados.

Responsabilidades devem ser definidas e cobradas de todos os colaboradores. Estas definições devem ser elaboradas de modo a não restringir totalmente o acesso aos meios, impossibilitando a execução das tarefas. Devem comunicar um consenso (SANS, 2002). Confiança deve ser a linha de ação na elaboração da política. Definir inicialmente quem poderá ter acesso a que e

quando. Políticas de segurança e procedimentos afetam todos em uma organização. As pessoas temem que estas políticas possam dificultar e complicar seu dia-a-dia de trabalho.

Administradores de rede acham mais cômodo trabalhar com políticas mais rígidas de segurança onde ocorram menos incidentes.

Algumas ilusões se disseminam sobre políticas de segurança, que são:

- Se utilizar as ferramentas certas, estarei seguro;
- Se for cuidadoso com o que utilizo, estarei seguro.

Os requerimentos básicos de uma política é que ela deve ser implementada, concisa e de fácil entendimento, ter razões para a existência de tal política, descrever o que cobre. Definir contatos, responsáveis e punições a serem tomadas (DIJKER, 1996).

Uma política de segurança é um conjunto de leis, regras e práticas que regulam como uma organização gerencia, protege e distribui suas informações e recursos.

Um dado sistema é considerado seguro em relação a uma política de segurança, caso garanta o cumprimento das leis, regras e práticas definidas nessa política.

Uma política de segurança deve incluir regras detalhadas definindo como as informações e recursos da organização devem ser manipulados ao longo de seu ciclo de vida, ou seja, desde o momento que passam a existir no contexto da organização até quando deixam de existir.

As regras que definem uma política de segurança são funções das designações de sensibilidade, associadas aos recursos e informações (por

exemplo: não classificado, confidencial, secreto e ultra-secreto), do grau de autorização das entidades (indivíduos ou processos agindo sob o comando de indivíduos) e das formas de acesso suportadas por um sistema.

A implementação de uma política de segurança baseia-se na aplicação de regras, que limitam o acesso de uma entidade às informações e recursos, com base na comparação do seu nível de autorização relativo a essa informação ou recurso, na designação da sensibilidade da informação ou recurso e na forma de acesso empregada. Assim, a política de segurança define o que é, e o que não é permitido em termos de segurança, durante a operação de um dado sistema. A base da política de segurança é a definição do comportamento autorizado para os indivíduos que interagem com um sistema.

- Política de Segurança Baseada em Regras: regras baseadas em atributos de sensibilidade genéricos; entidade com grau de segurança não classificado, confidencial, secreto ou ultra-secreto;
- Política de Segurança Baseada em Identidade: regras baseadas em atributos indivíduais específicos; o nome ou identificador da entidade no sistema.

A autorização em uma política de segurança baseada em regras normalmente apóia-se em informações sobre sensibilidade. Em um sistema seguro, os dados ou recursos devem ser marcados com rótulos de segurança que indicam o nível de sensibilidade. Os processos atuando sob o controle de indivíduos devem adquirir os rótulos de segurança apropriados, que definem o nível de autorização do indivíduo que o está controlando. As regras desse tipo de política utilizam os rótulos dos recursos e dos processos para determinar o tipo

de acesso que pode ser efetuado. No caso de uma rede de computadores, os dispositivos que implementam os canais de comunicação também possuem rótulos de segurança. Nesse caso, as regras que definem a política de segurança também determinam quando é, ou não, permitindo transmitir dados nesses canais, isto é, informações sensíveis só podem ser transmitidas em canais que ofereçam o nível de segurança adequado.

As políticas de segurança baseadas na identidade representam o tipo de controle de acesso mais encontrado nos computadores atuais. A base desse tipo de segurança é que um indivíduo, ou processo operando sob seu controle, pode especificar explicitamente os tipos de acesso que outros indivíduos podem ter às informações e recursos sob seu controle. O objetivo desse tipo de política é permitir a implementação de um esquema de controle de acesso que possibilite especificar o que cada indivíduo pode ler, modificar ou usar.

2.3.1. Controle de Acesso Físico

A segurança física pode ser abordada de duas formas:

- Segurança de acesso: que trata das medidas de proteção contra acesso físico não autorizado. Tem por objetivo proteger equipamentos e informações contra usuários não autorizados, prevenindo o acesso a esses recursos. Utilizam-se controles explícitos como fechaduras e cadeados, cujas chaves devem ser controladas.

- Segurança ambiental: que trata da prevenção de danos por causas naturais. Visam proteger os recursos computacionais contra danos provocados por desastres naturais, por falha da rede de fornecimento de energia. Os controles preventivos são a melhor atuação nestes casos.

3. AMEAÇAS E VULNERABILIDADES

3.1. Pontos Explorados

A evolução das redes de computadores identificou um importante equipamento de gerenciamento que é o servidor de redes. Sua função principal é prover serviço de comunicação, acesso e validação de usuários. Também é comum armazenarem dados valiosos para a organização. Não raro um único servidor de rede centraliza todos os dados da empresa, e ainda fornece acesso às outras máquinas a ele conectadas, faz papel de saída para acesso à rede mundial de computadores, Internet.

É consenso na área de segurança que as ameaças podem ter duas origens, internas e externas.

As ameaças internas, independente de estarem conectados ou não à Internet. Pode ser desde uma operação inadequada de um funcionário ou uma má configuração de um servidor de rede até o roubo da informação por funcionários da organização (MOREIRA, 2001). Alguns exemplos de ameaças internas são:

- Contaminação por vírus;
- Funcionários mal treinados;
- Divulgação de senhas;
- Funcionários de empresas terceirizadas.

As ameaças externas representam os ataques oriundos de fora do ambiente da organização, com objetivos de explorar as vulnerabilidades de um determinado sistema. Elas representam alto grau de participação nas pesquisas sobre ataques a sistemas computacionais.

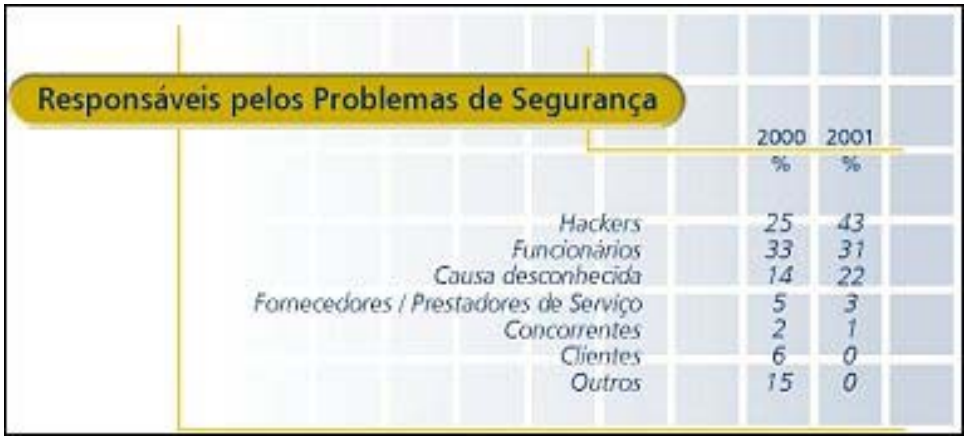

Figura 3.1: Responsáveis pelos problemas de segurança nas organizações. Fonte: 7ª Pesquisa Nacional sobre Segurança da Informação - Módulo Security Solutions (2001).

3.2. Potenciais Atacantes

O termo genérico para identificar quem realiza ataques em um sistema de computadores é hacker. Porém esta generalização possui diversas ramificações, pois cada ataque apresenta um objetivo diferente.

Por definição hackers são aqueles que utilizam seus conhecimentos para invadir sistemas, sem a intenção de causar danos às vítimas, mas como um desafio as suas habilidades. Os hackers possuem grande conhecimento de sistemas operacionais e linguagens de programação. Constantemente buscam

mais conhecimento, compartilham o que descobrem e jamais corrompem dados intencionalmente. (Segurança Máxima, 2000).

O termo hacker é definido pela RFC-2828 como sendo alguma pessoa com um grande interesse e conhecimento em tecnologia, não utilizando eventuais falhas de segurança descobertas em benefício próprio.

Como se tornou um termo genérico para invasores de redes, o termo hacker freqüentemente é usado para designar os elementos que invadem sistemas para roubar informações e causar danos. O termo correto para este tipo de invasores seria cracker ou intruder, que também é utilizado para designar aqueles que decifram códigos e destroem proteções de softwares (NAKAMURA e GEUS, 2002). Para Raymond (RAYMOND, 2000), crackers são pessoas que buscam lucros e benefícios próprios e rastreiam redes em busca de dinheiro, cartão de créditos e outros.

O termo cracker ou intruder é definido pela RFC-2828 como sendo alguém que tenta quebrar a segurança ou ganhar acesso a sistemas de outras pessoas sem ser convidado, não sendo, obrigatoriamente, uma pessoa com grande conhecimento de tecnologia como o hacker.

O termo hacker existe desde o final da década de 50. A palavra começou a ser usada pelos membros do Tech Model Rail Club, do Instituto de Tecnologia de Massachusetts (MIT), e indicava pessoas com capacidades técnicas para proezas que ninguém mais conseguia. Na área de informática este termo foi usado para designar programadores prodigiosos, tecnicamente superiores ao normal. Em 1988, em uma reportagem na CBS, rede de televisão americana, que

divulgava a conferência hacker, surgiu a conotação negativa da palavra hacker (Informática, 2002).

Uma classificação de diversos tipos de hackers pode ser a seguinte (Módulo Security Solutions, 1999):

- Script Kiddies: são iniciantes e executam programas encontrados na Internet já prontos não sabendo bem o que está acontecendo. É devido a eles que as organizações começaram a implementar políticas de segurança;
- Cyberpunks: mais velhos, porém anti-sociais, fazem invasões por divertimento e desafio, geralmente são os que encontram as vulnerabilidades em sistemas, protocolos ou serviços;
- Insiders: empregados insatisfeitos, responsáveis pelos incidentes mais graves financeiramente;
- Coders: os que escrevem ou divulgam em palestras suas proezas de invasões;
- White hat: profissionais contratados para descobrir falhas nos sistemas das empresas que contratam seus serviços;
- Black hat: também conhecidos por crackers ou Cyberterroristas, utilizam seus conhecimentos para invadir sistemas e roubar informações;
- Gray hat: hackers que vivem no limite entre white hat e black hat, podem passar informações a terceiros.

3.3. Técnicas Empregadas para Ataques

Embora as organizações estejam cada vez mais preocupadas com a segurança da informação e os investimentos na área venham aumentando, a freqüência dos ataques também vem crescendo em proporção desigual. Para se ter uma idéia do volume desses ataques, segue uma relação de tipos de técnicas empregadas por invasores de sistemas. (INFO Exame, 2000).

3.3.1. Cavalo de Tróia

Cavalo de Tróia ou trojan é um programa disfarçado que executa alguma tarefa maligna. Um exemplo: o usuário roda um joguinho que conseguiu na Internet. O joguinho instala o cavalo-de-tróia, que abre uma porta TCP do micro para a invasão. Este software não propaga a si mesmo, de um computador para outro. Alguns trojans populares são NetBus, Back Orifice e Sub7. Há também o cavalo de Tróia dedicado a roubar senhas e outros dados sigilosos.

3.3.2. Quebra Senha

O quebrador, ou cracker, de senha é um programa usado pelo hacker para descobrir uma senha do sistema. O método mais comum consiste em testar sucessivamente as palavras de um dicionário até encontrar a senha correta. Porém os processos modernos de

criptografia são de uma via e não existe nenhum processo para inverter a criptografia em um curto espaço de tempo.

3.3.3. Mail Bomba

É considerado como um dispositivo destrutivo. Utiliza a técnica de inundar um computador com mensagens eletrônicas. Em geral, o agressor usa um script para gerar um fluxo contínuo de mensagens e abarrotar a caixa postal de alguém. A sobrecarga tende a provocar negação de serviço (DoS) no servidor de e-mail. Raramente mails bomba culminam em perda de dados ou brechas de segurança, são ferramentas de molestamento.

3.3.4. Denial of Service (DoS)

Os ataques de negação de serviço são aborrecimentos semelhantes aos mails bomba, porém muito mais ameaçadores porque ataques DoS podem incapacitar temporariamente uma rede corporativa ou um provedor de acesso.

É um ataque que consiste em sobrecarregar um servidor com uma quantidade excessiva de solicitações de serviços. Sua finalidade não é o roubo de dados, mas tirar o site do ar. Há muitas variantes, como os ataques distribuídos de negação de serviço (Distributed Denial of Service - DDoS), que paralisaram sites como AMAZON, CNN, e-Bay,

Yahoo! , ZD Net e UOL em fevereiro de 2000. Nessa variante, o agressor invade muitos computadores e instala neles um software zumbi, como o Tribal Flood Network ou o Trinoo. Quando recebem a ordem para iniciar o ataque, os zumbis bombardeiam o servidor-alvo, tirando o servidor do ar.

3.3.5. Phreaking

É o uso indevido de linhas telefônicas, fixas e celulares. No passado, os phreakers empregavam gravadores de fita e outros dispositivos para produzir sinais de controle e enganar o sistema de telefonia. Conforme as companhias telefônicas foram reforçando a segurança, as técnicas tornaram-se mais complexas. Hoje o phreaking é uma atividade elaborada, que poucos dominam.

3.3.6. Scanners de Porta

São programas que buscam portas TCP abertas por onde pode ser feita uma invasão. Para que a varredura não seja percebida pela vítima, alguns scanners testam as portas de um computador durante muitos dias, em horários aleatórios.

3.3.7. Smurf

É um outro tipo de ataque de negação de serviço. O agressor envia uma rápida seqüência de solicitações de Ping (um teste para verificar se um servidor da Internet está acessível) para um endereço de broadcast. Usando spoofing, o cracker faz com que o servidor de broadcast encaminhe as respostas não para o seu endereço, mas para o da vítima. Assim, o computador-alvo é inundado pelo Ping.

3.3.8. Spoofing

É a técnica de se fazer passar por outro computador da rede para conseguir acesso a um sistema. Há muitas variantes, como o spoofing de IP. Para executá-lo, o invasor usa um programa que altera o cabeçalho dos pacotes IP de modo que pareçam estar vindo de uma outra máquina.

3.3.9. Sniffer

É um programa ou dispositivo que analisa o tráfego na rede. Sniffers são úteis para gerenciamento de redes. Mas nas mãos dos hackers permitem roubar senhas e outras informações sigilosas, uma vez que verificam todos os pacotes que trafegam pela rede.

Representam um risco significativo de segurança uma vez que não são facilmente detectáveis.

3.3.10. Vírus

São programas desenvolvidos para alterar softwares instalados em um computador, ou mesmo apagar todas as informações existentes no computador. Possuem comportamento semelhante ao do vírus biológico, multiplicam-se, precisam de hospedeiros, esperam o momento certo para o ataque e tentam se esconder para não serem exterminados. A internet e o correio eletrônico, são hoje as principais via de propagação de vírus.

A RFC-2828 define vírus como sendo um software com capacidade de se duplicar, infectando outros programas. Um vírus não pode se auto-executar, requer que o programa hospedeiro seja executado para ativar o vírus.

O ataque por vírus é o mais fácil de executar e o mais desastroso para o usuário. Os vários vírus desenvolvidos mensalmente fazem com que administradores de redes mantenham a estrutura de segurança atualizada, no que se refere a vírus. A sophos, empresa de antivírus atuando em todo o mundo, mantém estatísticas de ocorrências dos dez vírus mais reportados em 2002, conforme gráfico a seguir (SOPHOS, 2003).

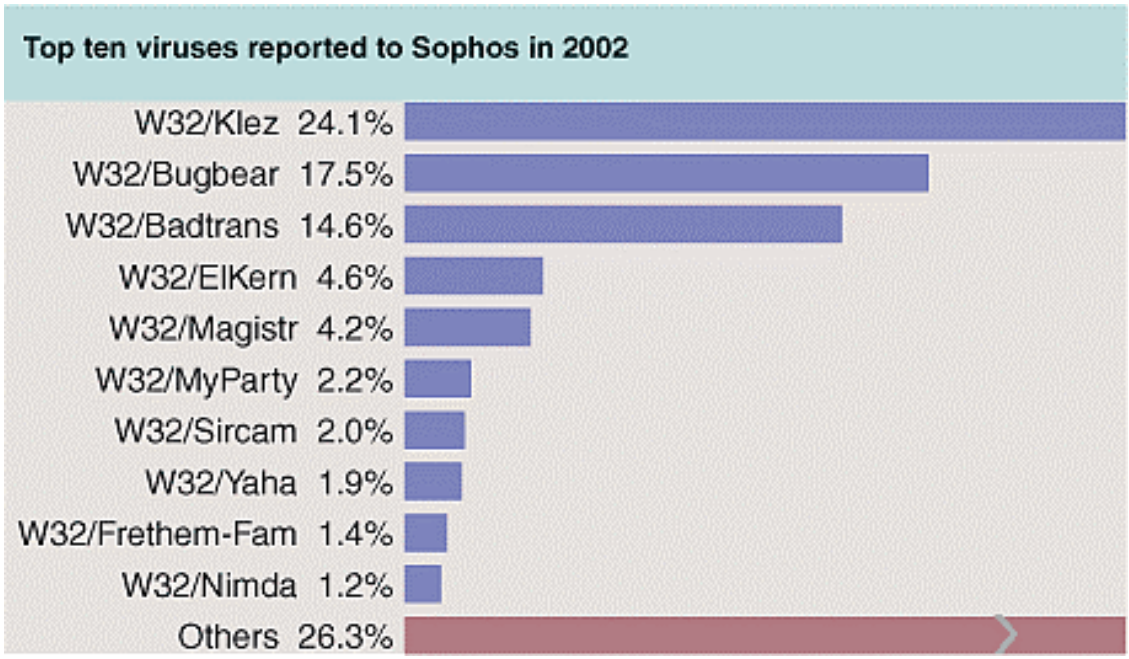

Figura 3.2: Dez vírus mais ativos em 2002. Fonte: SOPHOS Antivírus (www.sophos.com) (2003).

A sophos também divulgou estatística dos últimos seis meses, com os dez vírus mais ativos.

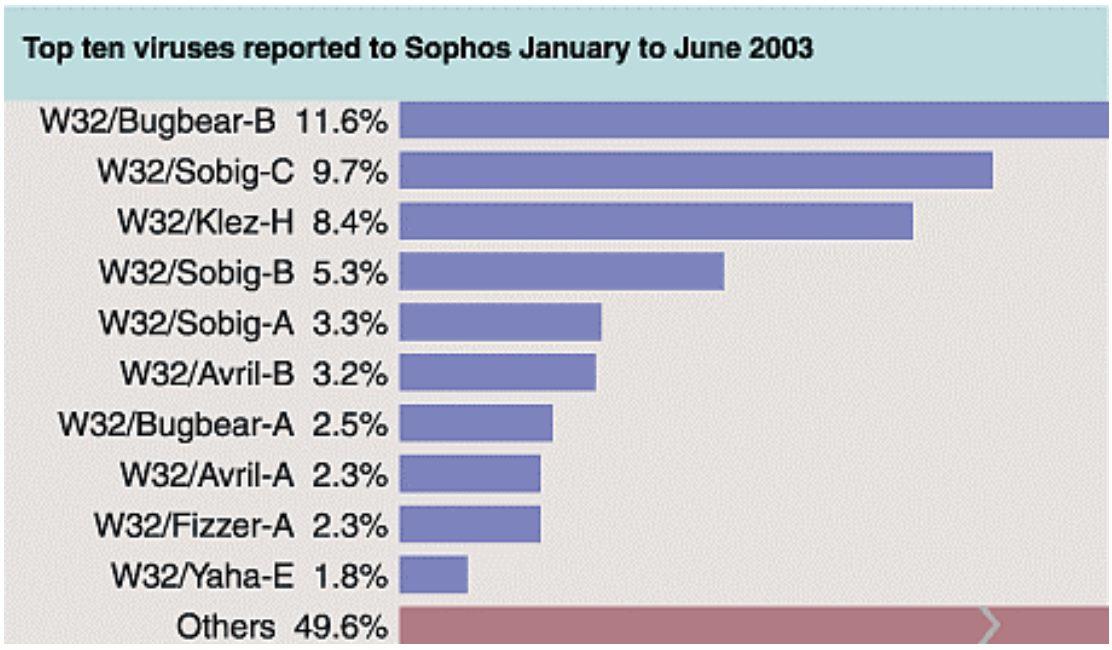

Figura 3.3: Dez vírus mais ativos no primeiro semestre de 2003. Fonte: SOPHOS Antivírus (www.sophos.com) (2003).

3.3.11. Worm

São programas auto-replicantes que não alteram arquivos, mas reside na memória ativa e duplica, a si mesmo, por meio de redes de computador. Os worms utilizam recursos do sistema operacional para ganhar acesso ao computador e ao se replicarem consomem recursos do sistema e tornam as máquinas lentas e interrompem outras funções. Alguns worms conhecidos são o *I love you, Nimda, Sircam, Cod Red II,* worms que em 2000 e 2001, em questão de horas, infectaram computadores na Europa e nas Américas, trazendo grandes prejuízos para os usuários da Internet.

A RFC-2828 define worm como sendo um programa de computador que pode se auto-executar, propagar-se pelos computadores de uma rede, podendo consumir os recursos do computador destrutivamente.

3.4. Ataques para Obter Informação (Coleta de Dados)

Existem diversas finalidades de ataques. O primeiro passo para um ataque é a obtenção de informações sobre o possível alvo. Conhecer o terreno e obter informações a respeito do alvo, é o primeiro passo para a realização de um

ataque bem sucedido. Após obter as informações sobre o alvo, o hacker pode atacar o sistema através de monitoramento da rede, infiltrar-se no sistema, inserir códigos nocivos ao sistema e colocar o sistema fora do ar. Duas técnicas para obter informações são o Trashing e a Engenharia Social. A primeira técnica consiste em vasculhar o "lixo" da empresa para verificar papéis amassados e jogados no lixo. Pode parecer loucura, mas esta técnica é bastante utilizada, inclusive no Brasil, onde casos com instituições financeiras já foram relatados.

Já a segunda técnica é mais direta, consiste em explorar as fraquezas humanas e sociais, fazendo com que a vítima entregue informações sem se aperceber deste fato. Um exemplo deste ataque consiste em uma pessoa se fazer passar por um alto funcionário da empresa que tem problemas de acesso ao sistema e necessita urgentemente acessar dados para seus compromissos.

Atuar sobre o colaborador/funcionário da organização é o meio mais eficiente de engenharia social. O colaborador/funcionário insatisfeito é o grande problema na falha de segurança das organizações. O roubo de informação por parte destes é hoje o maior índice de ocorrências registrados pelos órgãos de controle de acessos e invasões como o NIC BR Security Office (NBSO), o Centro de Atendimento a Incidentes de Segurança (CAIS-RNP), a Equipe de Segurança da UNICAMP, CERT-RS.

As organizações treinam e qualificam seus empregados, porém esquecem de motivar tais empregados para resguardar as informações manipuladas por eles no dia a dia (Módulo, 2002). Pesquisas efetuadas em 2001 pela empresa Módulo Security com organizações nacionais mostraram as principais ameaças às informações da empresa.

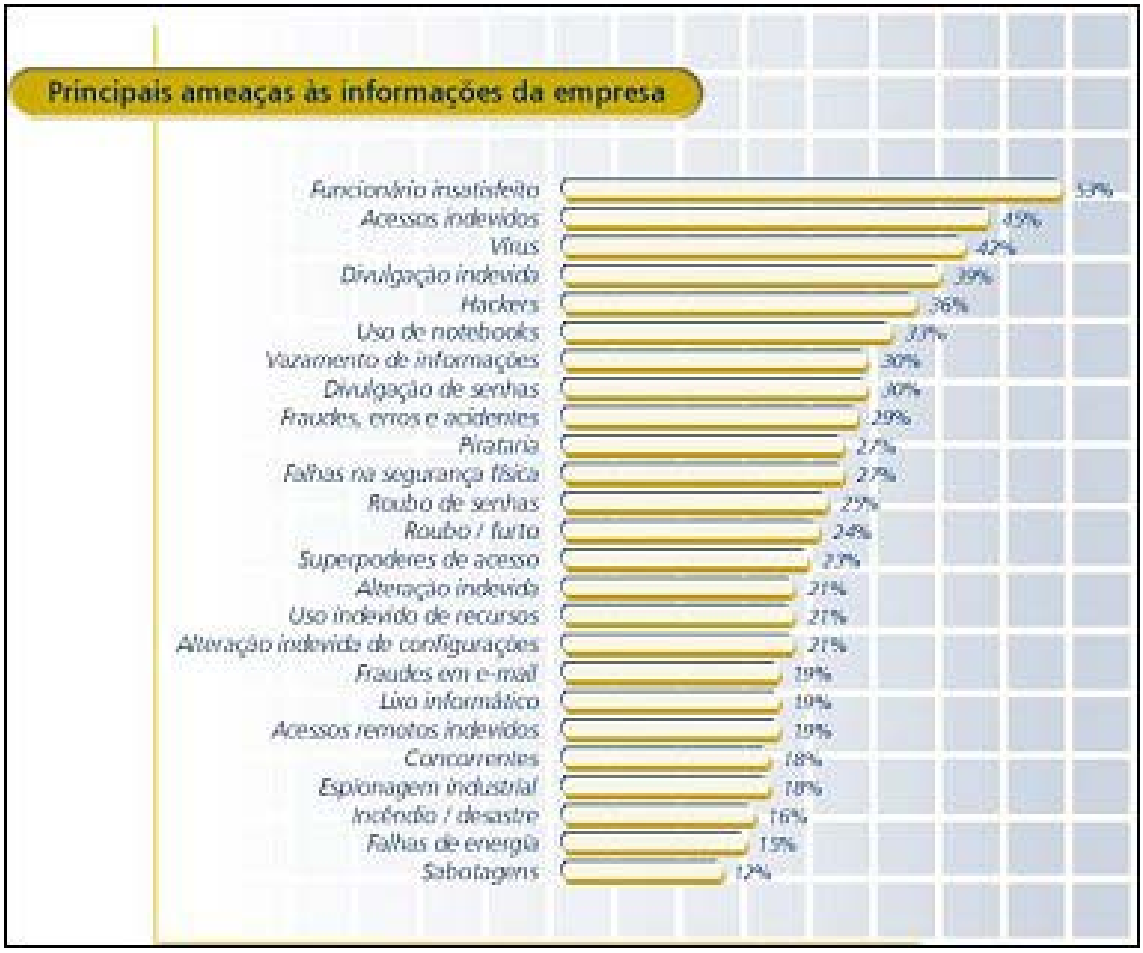

Figura 3.4: Principais ameaças às informações nas organizações. Fonte: 7ª Pesquisa Nacional sobre Segurança da Informação - Módulo Security Solutions (2001).

É grande a importância dos ataques originários a partir da rede interna da organização, feitos por funcionários ou ex-funcionários. Uma série de questões está envolvida com esse tema, desde a engenharia social até a relação do funcionário ou ex-funcionário com o chefe.

3.5. Ataques Físicos

O ataque físico à organização em que são roubados equipamentos ou softwares constitui um método menos comum. Este assunto também deverá fazer parte da discussão na elaboração da política de segurança, pois o acesso às dependências da organização deve ser controlado também.

3.6. Ataques de Negação de Serviço (Denial of Service – DoS)

Os ataques de negação de serviço fazem com que recursos sejam explorados de maneira agressiva, de modo que usuários legítimos ficam impossibilitados de utilizar os sistemas de rede. Uma técnica típica é o SYN Flooding que causa o estouro (overflow) da pilha de memória, por meio de envio de grande número de pedidos de conexão.

Diversas falhas (bugs) na implementação e na concepção de sérvios, aplicativos, protocolos e sistemas operacionais abrem “brechas” que podem ser exploradas.

3.7. Algumas Estatísticas sobre Ataques

No ano de 2001, segundo o Computer Emergency Response Team – Coordination Center (CERT/CC, 2001), da Carnegie Mellon University, houve grande prejuízo para as empresas norte-americanas por motivos de invasão de seus sistemas, por hackers ou crackers, e principalmente por vírus e worms. As organizações se descuidam da atualização de seus antivírus e ocorre muito mais estrago por meio destes que por uma invasão propriamente dito. Vírus como o

sircam, nimda, o code red e todas as suas variações fizeram grandes estragos. Tudo porque não houve uma atenção aos alertas divulgados pelas empresas fabricantes de antivírus. A atualização dos antivírus é coisa simples de ser feita, não requer muito conhecimento técnico por parte do usuário. Este é um treinamento que deve ser dado ao usuário final de qualquer máquina conectada à rede corporativa.

Em outra estatística realizada pelo CERT-CC, em 2001 houveram 52658 invasões reportadas nos Estados Unidos. No ano seguinte, 2002, este número aumentou para 82094 (CERT/CC, 2003). Na figura a seguir temos os registros reportados ao CERT/CC a partir de 1988.

Number of incidents reported

1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2002

Year	2000	2001	2002
Incidents	21,756	52,658	82,094

Total incidents reported (1988-2002): **182,463**

Figura 3.5: Número de incidentes reportados ao CERT/CC. Fonte: CERT/CC Statistics 1988-2002 (2003)

Em 2002, as ocorrências no Brasil foram maiores que no ano anterior. Segundo a pesquisa realizada pela empresa Módulo Security Solutions (MODULO, 2002), observa-se que a principal ameaça as informações das

organizações são os funcionários insatisfeitos, e em segundo vem o ataque por vírus. Porém nesta mesma pesquisa, 32 % dos entrevistados não sabiam informar se sofreram ataques e qual a incidência destes. Observou-se também que, ano após ano, cresce a preocupação das empresas nacionais com a proteção de suas informações, e aumenta também a adoção de controles para minimizar os riscos de ameaças e vulnerabilidades.

Segundo a pesquisa, as principais ameaças são funcionários insatisfeitos, disseminação de vírus e acessos indevidos, como mostra o gráfico abaixo.

Figura 3.6: Principais ameaças às informações nas organizações. Fonte: 8ª Pesquisa Nacional sobre Segurança da Informação - Módulo Security Solutions (2002).

Quanto a perdas financeiras, a pesquisa observou que as empresas começam a comunicar casos de invasão, mas ainda não conseguem, ou não divulgam, o montante de suas perdas, como mostra o gráfico a seguir.

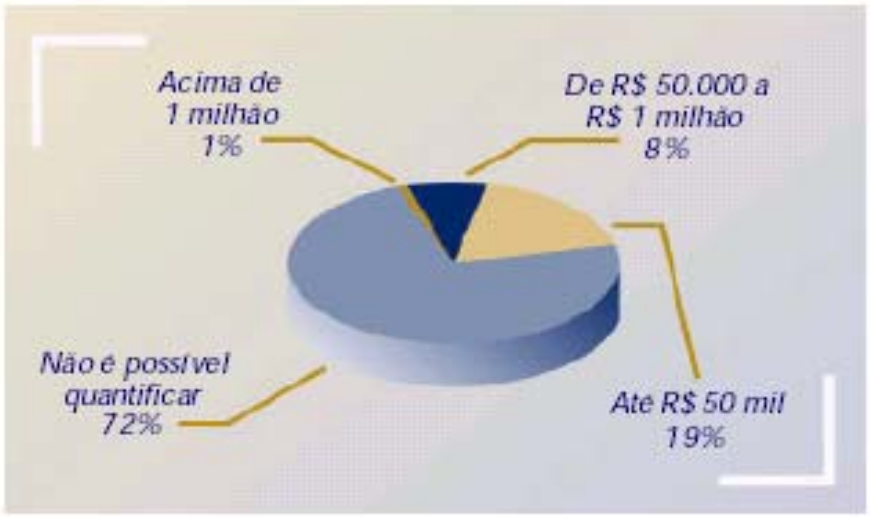

Figura 3.7: Quantificação de perdas com invasões nas organizações. Fonte: 8ª Pesquisa Nacional sobre Segurança da Informação - Módulo Security Solutions (2002).

Quanto à política de segurança, na sua maioria está desatualizada.

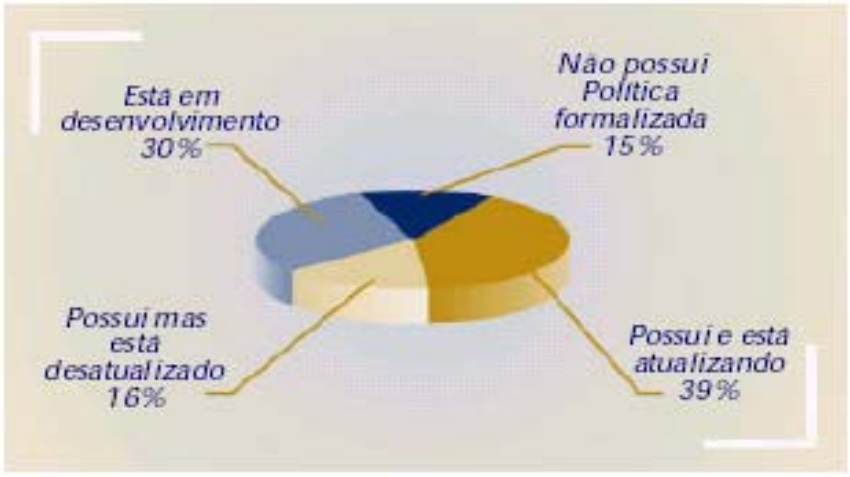

Figura 3.8: Política de Segurança. Fonte: 8ª Pesquisa Nacional sobre Segurança da Informação - Módulo Security Solutions (2002).

Um comparativo entre 2001 e 2002 quanto as principais medidas de segurança adotadas, podemos observar que o antivírus ainda é a medida mais adotada.

Figura 3.9: Principais medidas de segurança adotadas. Fonte: 8ª Pesquisa Nacional sobre Segurança da Informação - Módulo Security Solutions (2002).

No Brasil existem alguns grupos de segurança e resposta a incidentes, que fazem levantamento sobre as ocorrências na internet brasileira. Estes organismos são:

- Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Pesquisa (CAIS-RNP): atende redes de instituições de ensino superior, institutos de pesquisa e similares conectados ao backbone da RNP;
- Computer Emergency Response Team – Rio Grande do Sul (CERT-RS): atende a redes do domínio Tche.br e clientes do ponto de presença (POP)-RS/RNP no Rio Grande do Sul;

- Centro de Tratamento e Resposta a Incidentes em Redes do Departamento de Polícia Federal (CTR): atende redes de domínios federais e de interesse da União;
- Empresa Brasileira de Telecomunicações (EMBRATEL): atende redes conectadas à Embratel;
- Equipe de Segurança de Redes e Resposta a Incidentes da Universidade de São Paulo – USP: atende redes de endereços IP e domínios alocados à Universidade de São Paulo;
- Equipe de Segurança em Sistemas e Redes da Universidade Estadual de Campinas – UNICAMP: atende redes de endereço IP e domínios alocados para a Universidade Estadual de Campinas;
- Grupo de Segurança de Redes do Instituto Nacional de Pesquisas Espaciais (GSR/INPE): atende redes de endereço IP e domínios alocados para o Instituto Nacional de Pesquisas Espaciais/Brasil;
- NIC BR Security Officer – Brazilian Computer Emergency Response Team (NBSO): atende redes de domínios sob o TDL.br e endereços IP alocados para o Brasil;
- Star One: atende redes de endereços IP alocados à Star One e domínios easyband.com.br, e outros.

O Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Pesquisa (CAIS-RNP), relatou um aumento de 82% nos incidentes reportados ao organismo, passando de 7.209 para 12.114 (CAIS/RNP, 2003).

Dentre os incidentes notificados, se destacaram as atividades de reconhecimento (scanner) direcionadas aos serviços comuns de acesso à internet que são o SSH, FTP, HTTP. Depois aparecem as trocas de páginas, uso indevido de servidores FTP para repositório de filmes e músicas, e envio de spam. A seguir observamos o gráfico das estatísticas levantado pelo CAIS-RNP.

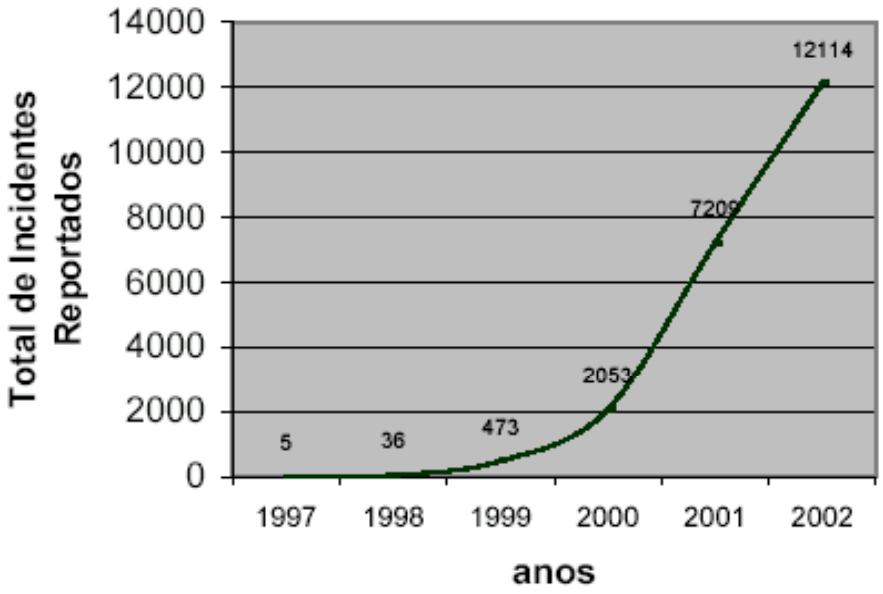

Figura 3.10: Comparativo de incidentes reportados ao CAIS. Fonte: CAIS/RNP Relatório Anual (2002).

Um dos destaques observados pelo CAIS foram os vírus W32.Klez e suas variantes, o worm JS/SQL.Spida.b.worm, o Slapper, o W32.BugBear e o OpaServ.

A NIC BR Security Officer (NBSO) também mantém um registro de ocorrências da internet brasileira. No ano de 2002 teve um total de 25092 ocorrências distribuídas da seguinte maneira.

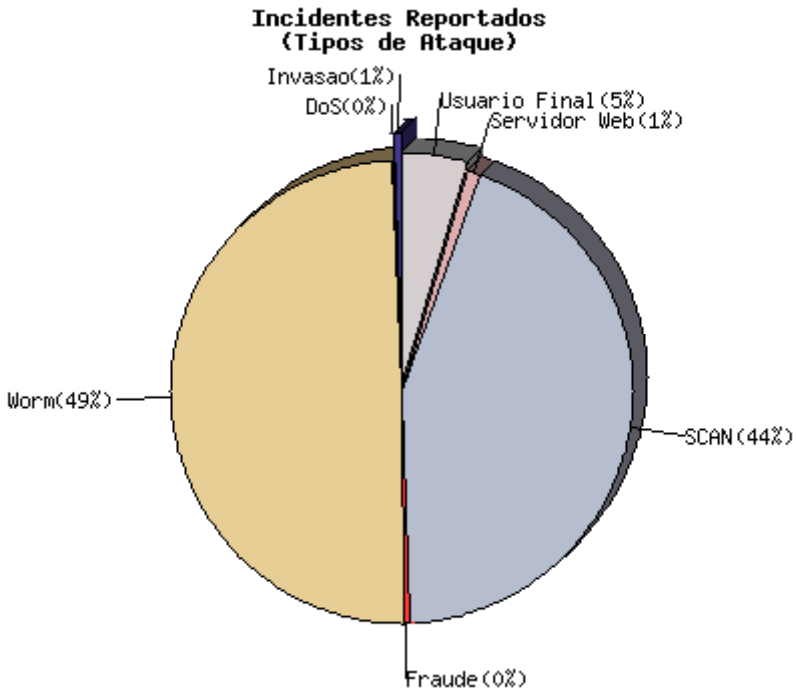

Figura 3.11: Incidentes reportados ao NBSO em 2002. Fonte: NBSO Estatísticas de Incidentes Reportados ao NBSO (2003).

Nos seis primeiros meses deste ano de 2003, obtiveram dois gráficos com as ocorrências, conforme segue.

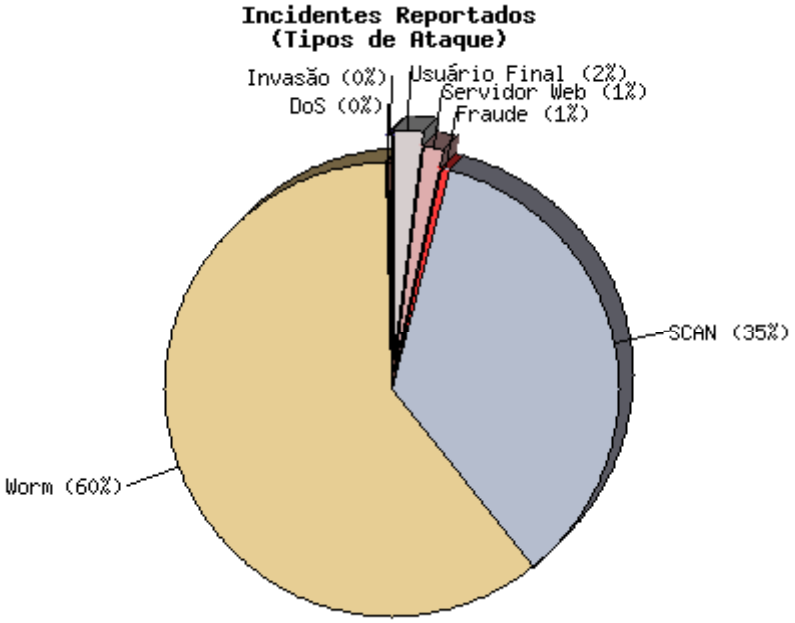

Figura 3.12: Incidentes reportados ao NBSO de janeiro a março de 2003. Fonte: NBSO Estatísticas de Incidentes Reportados ao NBSO (2003).

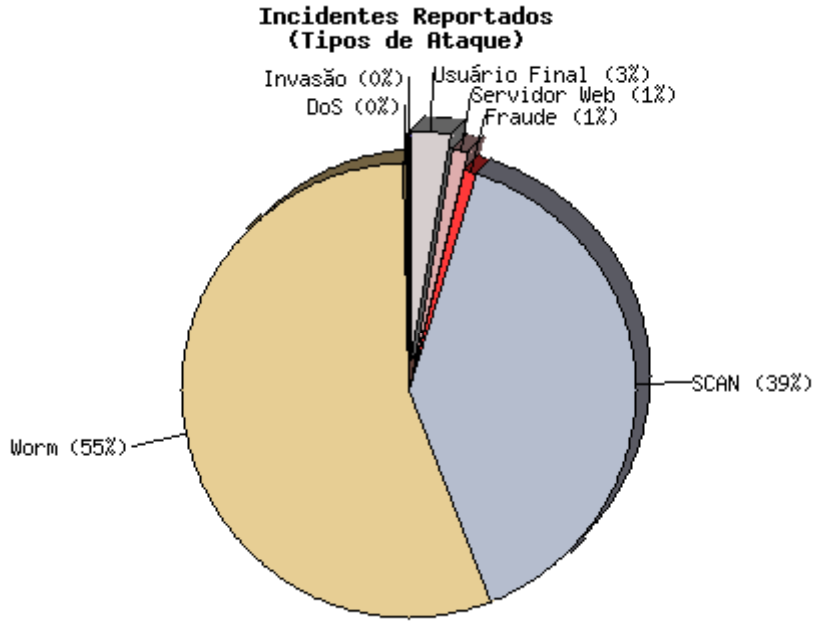

Figura 3.13: Incidentes reportados ao NBSO de abril a junho de 2003. Fonte: NBSO Estatísticas de Incidentes Reportados ao NBSO (2003).

As pesquisas feitas em 2002, pelo CSI/FBI, mostraram que 90% das organizações americanas detectaram falhas nos sistemas de segurança de seus computadores. Destes, 80% admitiram ter sofrido prejuízos financeiros e 44% declararam perdas da ordem de 456 milhões de dólares, aproximadamente 20% a mais que em 2001 (CSI - Computer Security Institute e FBI - Federal Bureau of Investigation's – 2002).

Até metade de 2003 várias ocorrências já foram registradas. Na pesquisa realizada pelo CSI/FBI, é feita uma comparação entre anos anteriores, com relação aos incidentes reportados na pesquisa. Com relação ao ponto inicial de ataque, isto é, de onde vem a maioria dos ataques, observou-se que é através da internet, seguido de ataques a sistemas internos e por fim acesso à rede através de conexão discada.

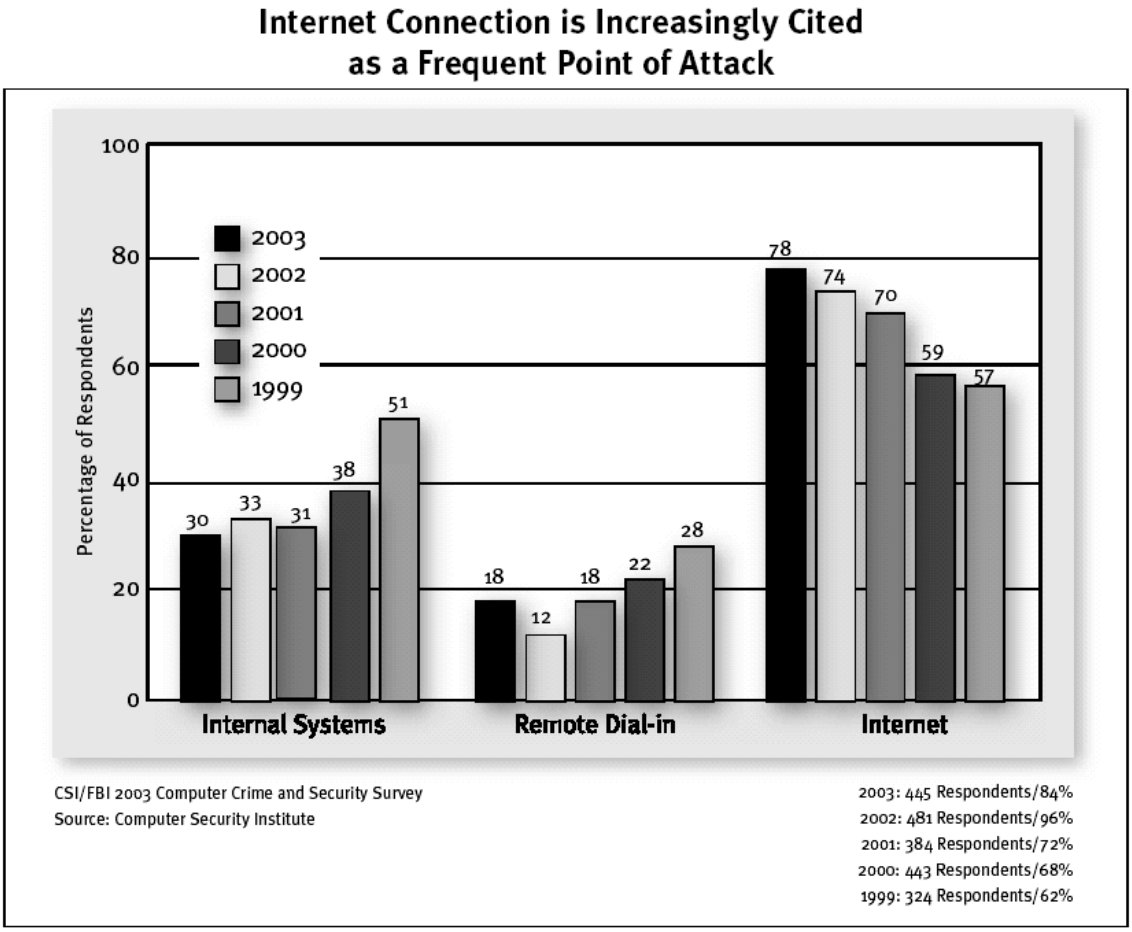

Figura 3.14: Ponto freqüente de ataque. Fonte: CSI/FBI 2003 Computer Crime and Security Survey (2003).

A fonte dos ataques é, segundo a pesquisa, liderada por empregados insatisfeitos com a organização, e hackers. Estes últimos na liderança com uma pequena folga.

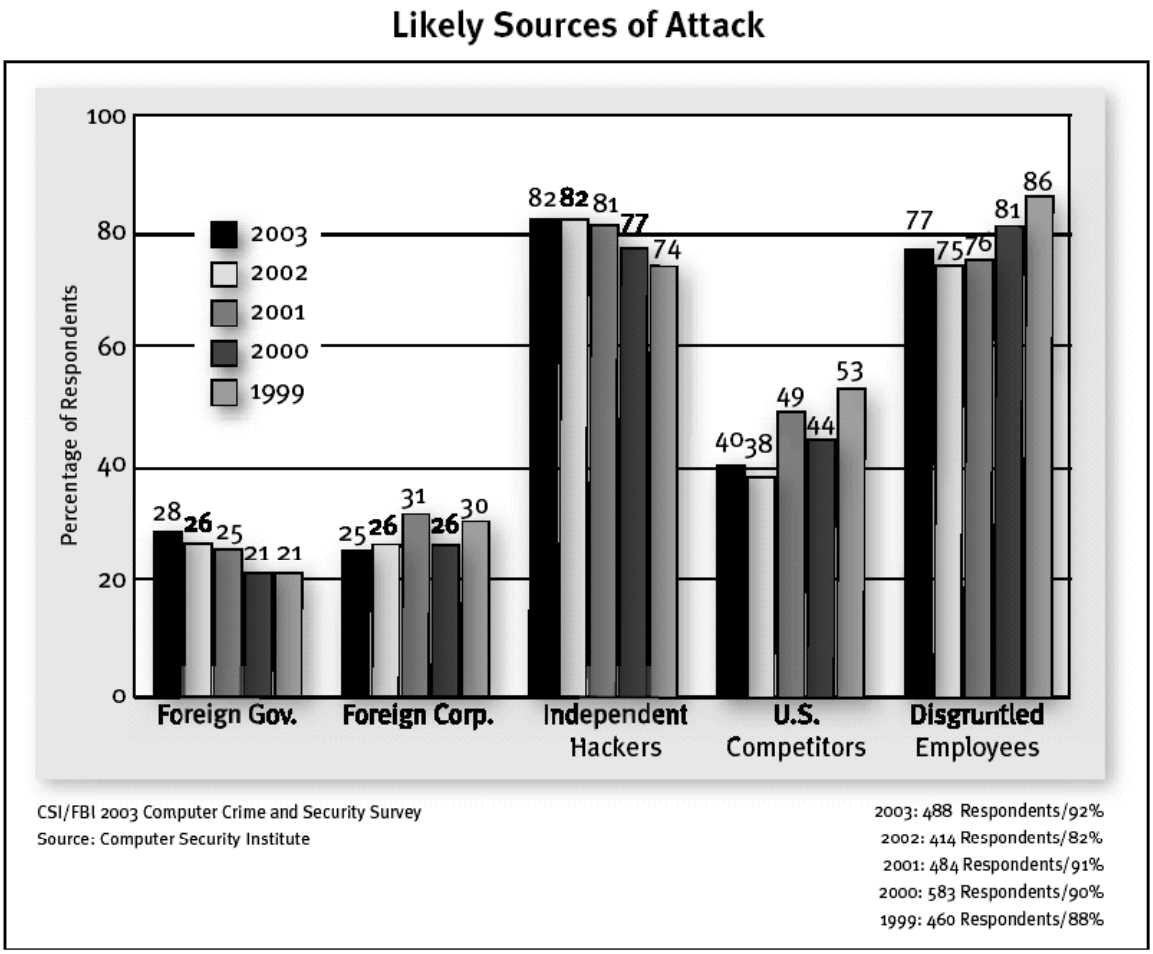

Figura 3.15: Fonte dos ataques. Fonte: CSI/FBI 2003 Computer Crime and Security Survey (2003).

E também observamos que os vírus lideram os tipos de ataques, seguidos de invasões internas.

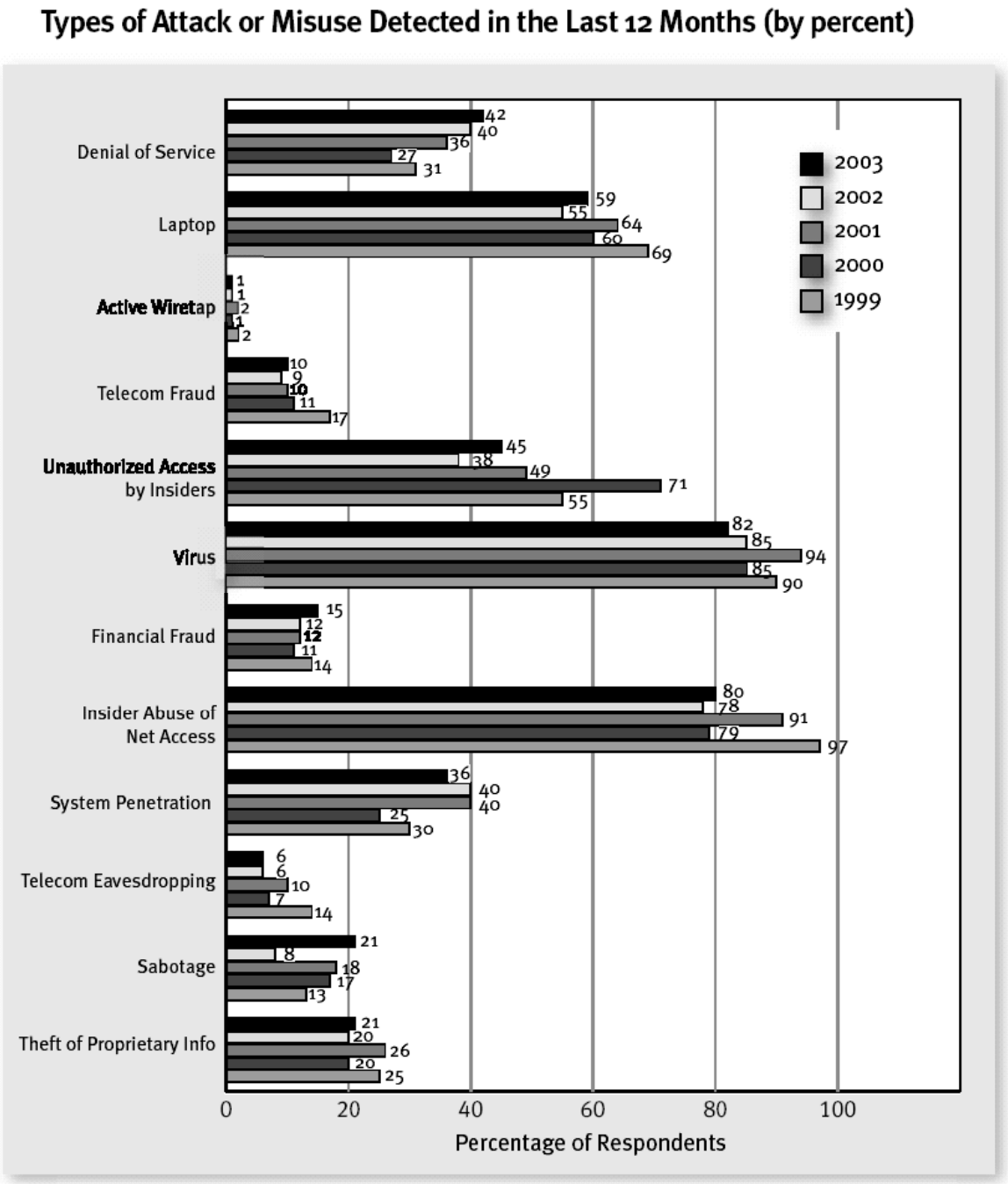

Figura 3.16: Tipo dos ataques. Fonte: CSI/FBI 2003 Computer Crime and Security Survey (2003).

4. PREVENÇÃO E PROTEÇÃO CONTRA ATAQUES

4.1. Alguns Mecanismos de Proteção

Algumas tecnologias de segurança não serão abordadas neste trabalho, porém deve se registrar que, levando-se em consideração as pesquisas realizadas com empresas americanas e brasileiras pelos diversos organismos que mensuram os incidentes na internet, podemos mostrar algumas citadas nos relatórios.

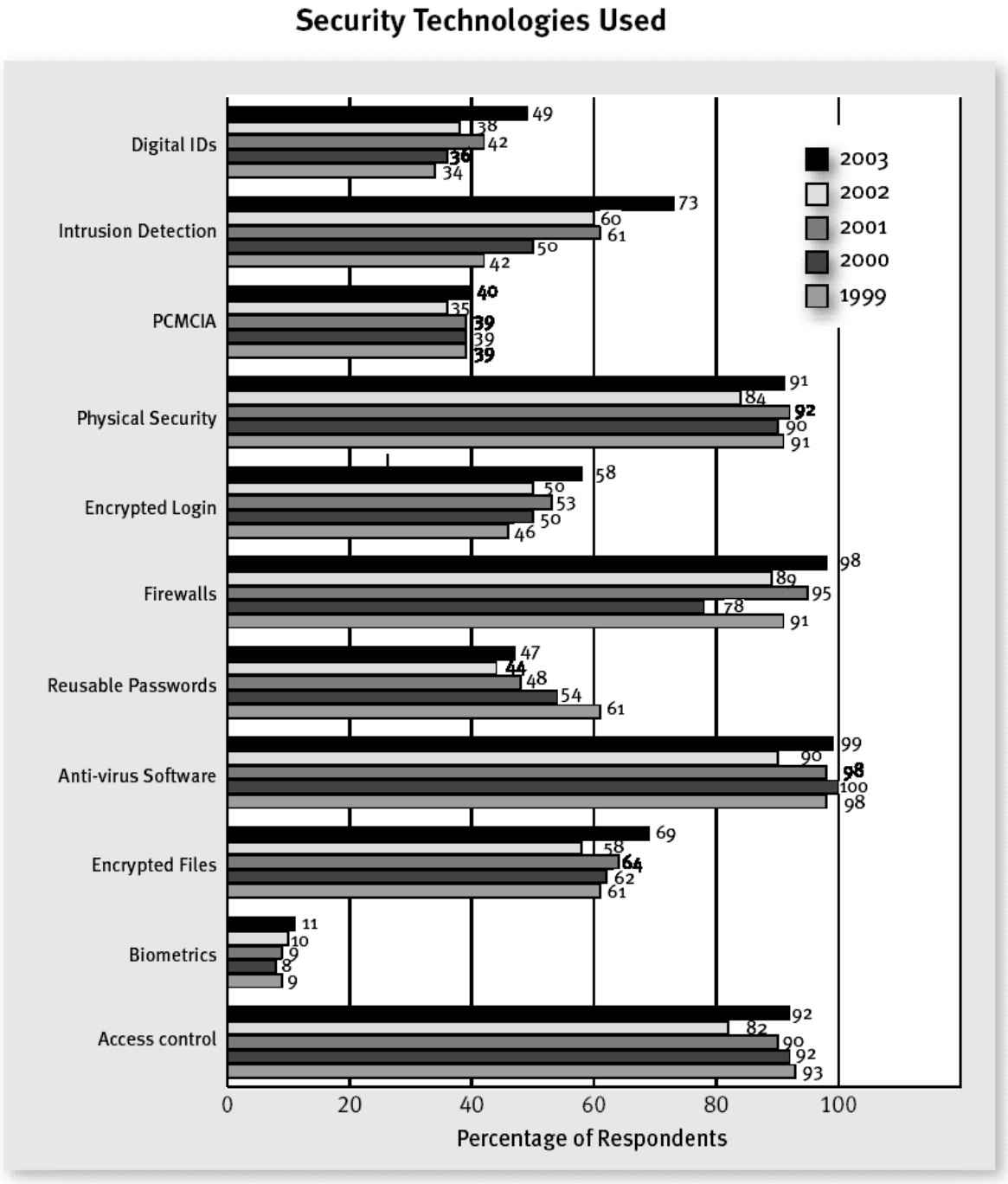

Figura 4.1: Tipo de tecnologias de segurança. Fonte: CSI/FBI 2003 Computer Crime and Security Survey (2003).

4.1.1. Firewall

A RFC-2828 define o termo firewall como sendo uma ligação entre duas redes de computadores que restringem o tráfego de comunicação de dados entre a parte da rede que está “dentro” ou “antes” do firewall, protegendo-a das ameaças da rede de computadores que estão “fora” ou depois do firewall.

Um firewall é um sistema ou conjunto de sistemas através do qual flui o tráfego de dados entre duas redes distintas de computadores, permitindo que se implemente uma política de segurança que determine o que pode ou não passar de uma rede para outra. Os firewalls são controles de acesso externo à rede, e podem oferecer proteção contra ataques a protocolos ou aplicações individuais, protegem contra ataques spoofing e têm relativa flexibilidade de configuração, oferecendo vários tipos de configurações e de restrições para diferentes tipos de tráfego.

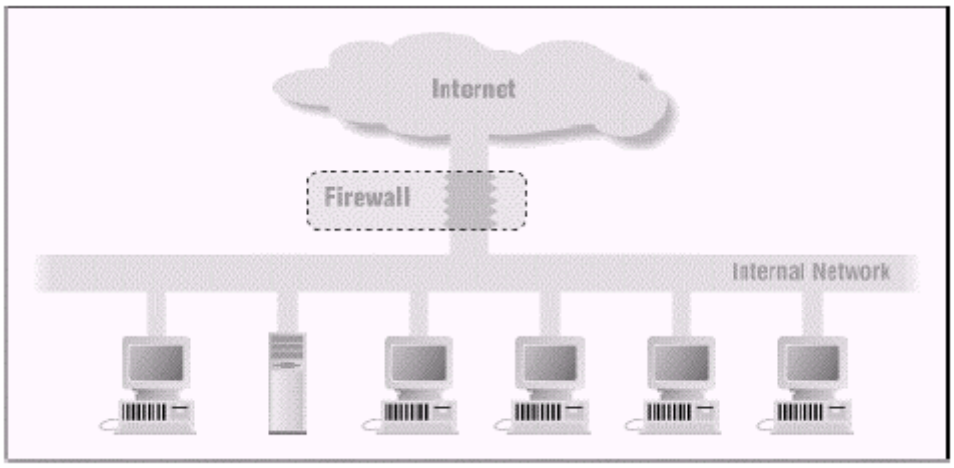

Figura 4.2: Posicionamento do firewall na rede de computadores. Fonte: ZWICKY et al, (2000).

O firewall determina quais são os serviços de rede que podem ser acessados, dentro desta mesma rede, por usuários que estão fora da rede. Para que seja seguro, todo o tráfego de informação através da internet deverá passar pelo firewall, caso o invasor consiga passar pelo firewall este já não terá utilidade de proteção (MADRIGAL, 2000).

Porém um firewall não pode proteger contra ataques que se efetuam fora de sua área de abrangência, isto é claro. Por exemplo, se dentro de sua rede interna existe uma conexão de acesso discado (dial-up) sem restrições, que permita acessar à rede interna através desta conexão evitando assim o firewall. Este tipo de conexão evita o acesso ao firewall criando uma porta de ataque sem restrições ou controle (MADRIGAL, 2000).

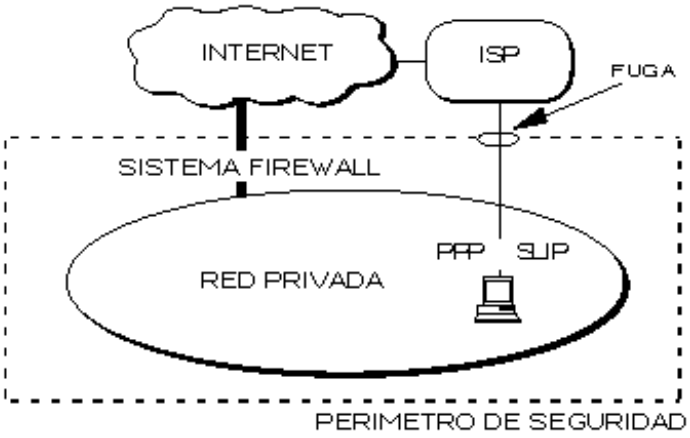

Figura 4.3: Exemplo de conexão anexa ao firewall Fonte: MADRIGAL, (2000).

Fisicamente um firewall pode ser um dispositivo de hardware dotado de duas ou mais placas de rede (uma ligada à rede interna e outra à rede externa), rodando softwares específicos de análise e roteamento de pacotes. Como todo

pacote enviado de uma rede a outra passa pelo sistema, o firewall tem a chance de analisá-lo, verificando se representam riscos para a rede interna.

Alguns firewalls dão maior ênfase ao bloqueio de tráfego e outros trabalham na permissão do tráfego por eles.

Existem duas políticas básicas para implementação de um firewall:

- Default Permit: qualquer host ou protocolo que não esteja dentro do conjunto de regras que irão resultar no bloqueio dos dados será permitido por default;
- Default Deny: essa política permite a passagem ou o acesso a subrede, somente os especificados na política.

Em geral as empresas utilizam três tipos de firewalls (BERNSTEIN et al., 1997) que são os filtros de pacotes baseados no roteador e no host, filtros inteligentes baseados no host, e gateways/proxy de aplicações baseadas no host.

Algumas arquiteturas ou topologias mais comuns também são definidas por Allen (ALLEN, 2001) que são:

- Firewall de Borda: é o básico de todos os firewalls. Consiste em uma conexão de um computador da rede interna da organização com alguma outra rede não confiável ou não administrada pelo pessoal interno da organização, tipicamente a Internet. Este computador faz todas as funções de firewall;

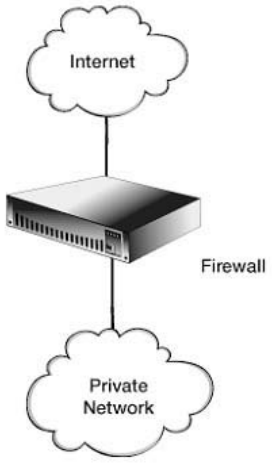

Figura 4.4: Arquitetura de Firewall de Borda. Fonte: ALLEN, (2001).

- Computador não Confiável (Untrustworthy host): baseado no firewall de borda, somente adiciona um computador entre o firewall e a rede não confiável, fora da atuação do firewall. Este computador é configurado e gerenciado com a maior segurança possível, e o firewall é configurado pra verificar tanto pacotes que entram como os que saem da rede interna da organização, e devem necessariamente passar pelo equipamento colocado fora do firewall;

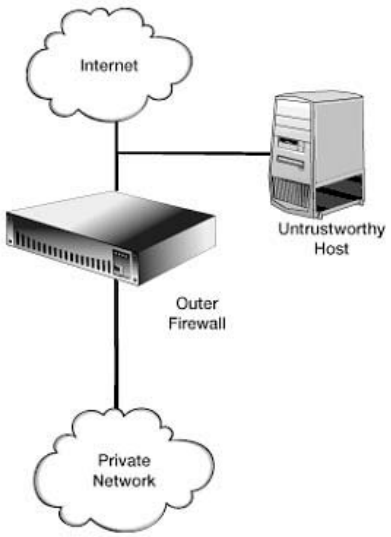

Figura 4.5: Arquitetura de Firewall com Computador não confiável (untrustworthy). Fonte: ALLEN, (2001).

- Rede Desmilitarizada (DMZ): o computador não confiável é colocado dentro da abrangência do firewall, criando uma rede de um só computador, assim o firewall atua sobre três redes distintas. Isto aumenta a segurança, confiabilidade e a disponibilidade do computador não confiável, mas não aumenta o nível de confiança dos computadores dentro da rede;

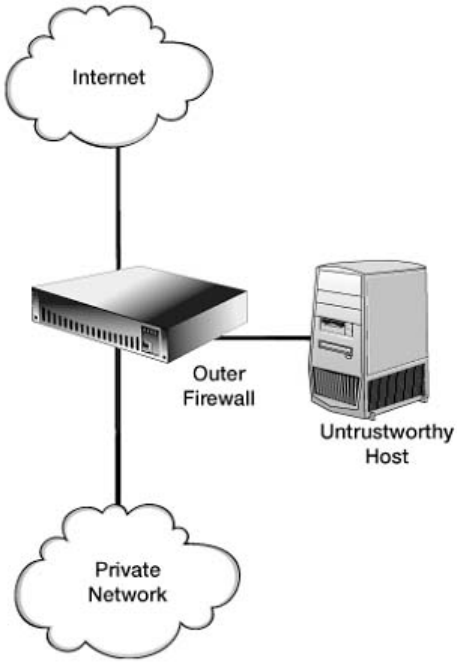

Figura 4.6: Arquitetura Básica de Firewall baseada em redes DMZ. Fonte: ALLEN, (2001).

- Dual Firewall: a rede interna da organização é isolada da rede não confiável adicionando-se um segundo equipamento de firewall. O tráfego de informações da rede interna da organização para fora dela, será vistoriado pelos dois firewalls e pela rede desmilitarizada (DMZ).

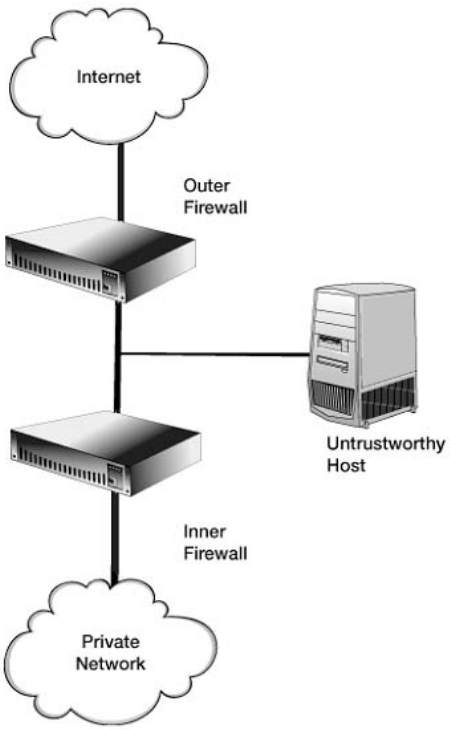

Figura 4.7: Arquitetura Dual Firewall com rede DMZ. Fonte: ALLEN, (2001).

Em cada uma destas arquiteturas o firewall será usado como controlador de acesso à rede interna da organização com propósitos de proteção da rede (ALLEN, 2001). O controle de sub-redes dentro da organização pode ser feito através de firewalls da mesma forma como explicado anteriormente.

4.1.2. Criptografia

A RFC-2828 define o termo criptografia como a ciência matemática que trabalha com a transformação de dados para mudar seu significado em algo ininteligível para o inimigo, isto é, esconder o seu conteúdo semântico,

prevenindo a sua alteração ou o seu uso sem autorização. Se a transformação é reversível, a criptografia também trata da restauração dos dados codificados para uma forma inteligível. Carvalho (2000) define origem grega da palavra criptografia (Kriptos = escondido, oculto e Graphia = escrita), que consiste na arte ou na ciência de escrever em cifras ou em códigos, utilizando um conjunto de técnicas que torna uma mensagem incompreensível, chamada comumente de texto cifrado, através de um processo chamado cifragem, permitindo que apenas o destinatário desejado consiga decodificar e ler a mensagem. Talvez tão antiga quanto à própria escrita, hoje é um dos métodos mais eficientes de se transferir informações sigilosas.

Guttman e Bagwill (1997) salientam que a criptografia é o meio primário para oferecer confidencialidade às informações transmitidas entre as redes de computadores ou através da Internet.

Existem diversas técnicas de criptografia utilizadas como meio de proteção das informações armazenadas ou trafegando pelas redes, que visam prover uma comunicação segura entre máquinas, garantindo sua privacidade. A criptografia emprega algoritmos e chaves. Os algoritmos são regras ou funções matemáticas para a alteração dos dados. As chaves são parâmetros ou variáveis utilizadas pelos algoritmos para criptografar os dados (MARQUES, 2001).

Os algoritmos de criptografia fazem uso de uma chave para controlar a codificação e a decodificação. As chaves são elementos fundamentais que interagem com os algoritmos, como mostrado a seguir (TRINTA e MACEDO, 2000).

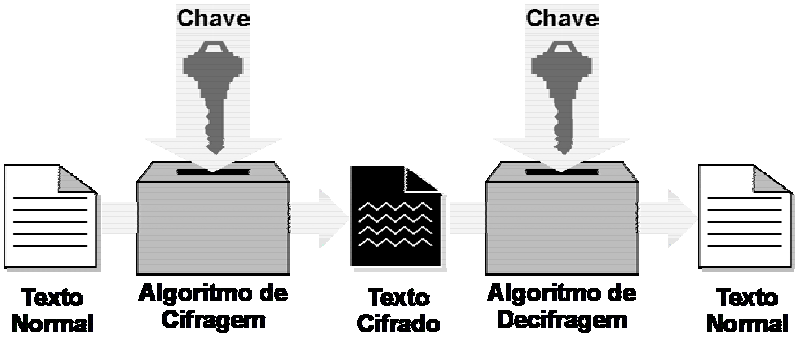

Figura 4.8: Utilização das chaves nos algoritmos criptográficos. Fonte: TRINTA e MACEDO (2000).

Uma chave é uma cadeia aleatória de bits utilizada em conjunto com um algoritmo. Cada chave distinta faz com que o algoritmo trabalhe de forma ligeiramente diferente (MAIA, 2000).

O uso de chaves na criptografia refere-se ao acesso a informações cifradas, devendo o usuário possuir a chave correta para poder decodificar a mensagem. Os tipos de criptografia são os de chaves simétricos e os de chaves assimétricos explicados a seguir:

- Criptografia de Chave Assimétrica: esta é a criptografia tradicional onde a mesma chave que codifica também decodifica a mensagem. Este método também é conhecido como chave privada e utiliza uma chave única. Uma de suas características (NAKAMURA, 2000) é sua rapidez, porém não permitem a assinatura nem a certificação digital. Existe também uma desvantagem, para o destinatário conseguir ler a mensagem o emissor deverá enviar, antecipadamente, a mesma chave para decifrar a mensagem, tornando-se assim um método inseguro caso não seja utilizada uma conexão segura para enviar a chave.

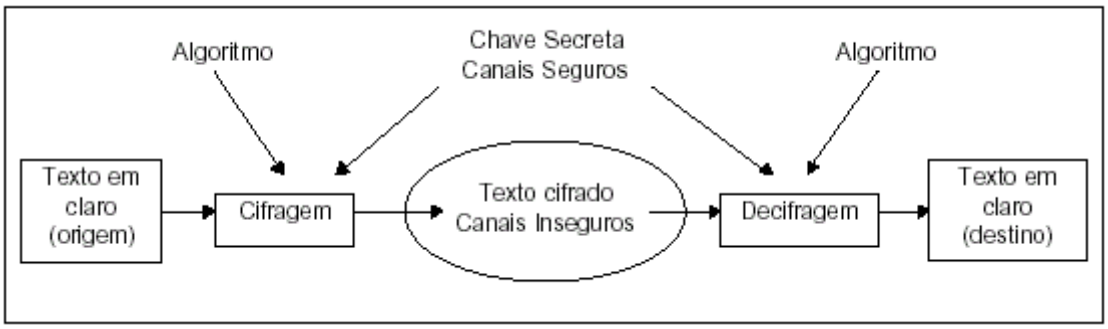

Figura 4.9: Modelo de Criptografia de Chave Simétrica ou Privada.

- Criptografia de Chave Assimétrica: é a utilização mais comum e funciona com duas chaves, uma para codificar chamada de chave pública e outra para decodificar a mensagem chamada de chave privada. A criptografia de chave assimétrica também é conhecida como de chave pública. As duas são geradas ao mesmo tempo e guardam uma relação entre si. A chave pública é distribuída entre os remetentes da mensagem e a privada permanece somente com o destinatário, a que circula pela rede é a chave pública. Quando chega ao destino, é utilizada a chave privada para decodificar a mensagem. As chaves públicas permitem a autenticação através da assinatura digital e da certificação digital, porém ao contrário da criptografia de chave privada, este método é mais lento.

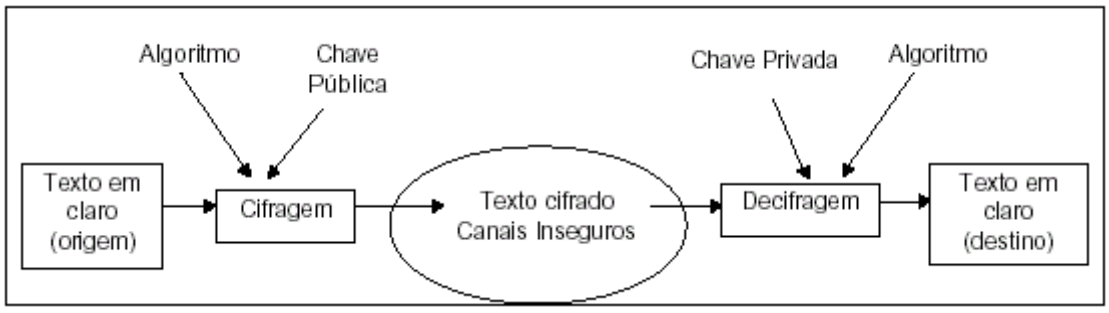

Figura 4.10: Modelo de Criptografia de Chave Assimétrica ou Pública.

No desenho acima, a chave pública está para cifragem e a chave privada para decifragem, poderia ser ao contrário o que caracteriza uma assinatura digital.

A utilização de sistemas criptográficos tem crescido muito e, devido a sua importância, os fatores que podem causar falhas na criptografia devem ser considerados (SCHNEIER, 1998). Estas falhas podem ser:

- Falha na checagem do tamanho de valores;
- Reutilização de parâmetros aleatórios, que não devem ser reutilizados;
- Alguns sistemas não destroem a mensagem em texto simples, depois de ser feita a codificação;
- Há falhas na utilização da base de dados de recuperação de chaves em casos de emergência.

Essas falhas podem ser exploradas por meio de ataques feitos por hardware, que podem introduzir falhas no processamento criptográfico (SCHNEIER, 1998).

4.1.3. Assinatura Digital

Quem utiliza a internet para efetuar negócios ou estabelecer relações comerciais, o quesito segurança é o que mais preocupa, pois poderá

comprometer qualquer tipo de negociação se não for bem administrada pelas partes envolvidas.

Um dos mecanismos utilizados na internet para garantir negociações seguras é a assinatura digital, que tem como objetivo garantir a veracidade de um documento que está circulando pela rede. Este artifício decorre da necessidade de, posteriormente, provar a um terceiro participante da negociação, que esta se realizou de boa fé e tem veracidade legal.

Assinatura Digital é um conjunto de procedimentos matemáticos realizados com a utilização de técnicas de criptografia assimétrica que permite a comprovação da autoria. O mecanismo de assinatura digital envolve dois procedimentos:

- Que o receptor possa verificar a identidade declarada pelo transmissor (assinatura);
- Que o transmissor não possa, mais tarde, negar a autoria da mensagem (verificação).

O procedimento da assinatura envolve a codificação da unidade de dados completa ou a codificação parcial.

O procedimento de verificação envolve a utilização de um método e uma chave pública para determinar se a assinatura foi produzida com a informação privada do signatário.

A padronização da assinatura digital feita pelo NIST (National Institute of Standards and Technology - USA) através da FIPS PUB 186 (1991, 1993,1996), a DSS (Padrão de Assinatura Digital), usa o Algoritmo Hash Seguro (SHA), que é a geração de código hash e algoritmos de chave pública. A assinatura é obtida

aplicando uma função de hash na mensagem, assim obtém-se um valor hash para a assinatura; o qual é criptografado e utilizando uma chave privada do autor, é adicionado ao documento e o enviado. Em seguida, criptografa a mensagem junto com sua assinatura, utilizando a chave pública do receptor. Este, ao receber a mensagem, deve, primeiramente, decifrá-la com sua chave privada, o que garante sua privacidade. Em seguida, decifrá-la novamente, para verificar a assinatura utilizando a chave pública do autor, garantindo assim sua autenticidade.

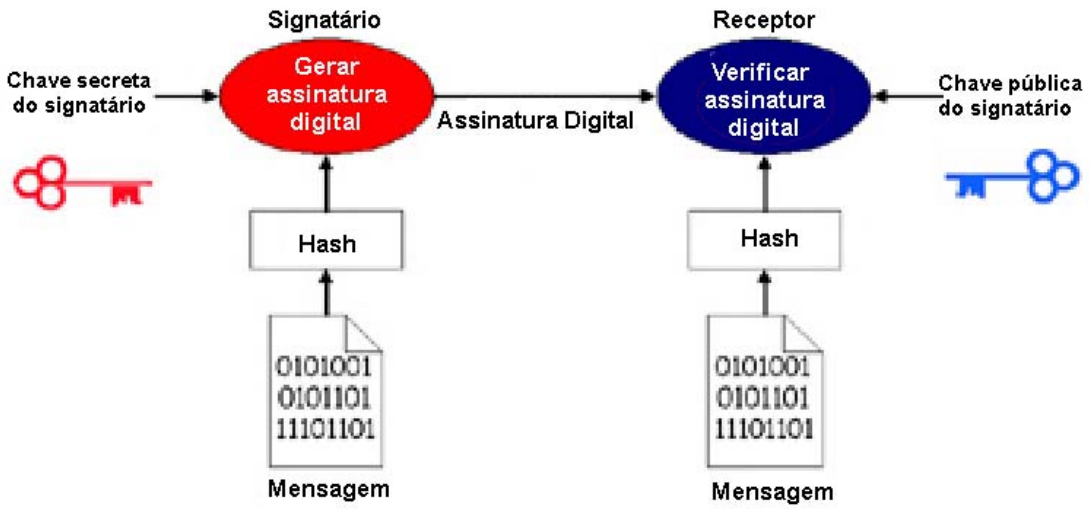

Figura 4.11: Geração de uma assinatura digital.

4.1.4. Certificado Digital

O Certificado Digital associa a identidade de um titular a um par de chaves eletrônicas que usadas em conjunto comprovam a identidade de determinada entidade ou pessoa. O certificado é emitido e assinado por uma entidade

certificadora. Tem por objetivo assegurar a transmissão de dados entre organizações.

Um certificado contém três elementos:

- Informação de atributo: que são informações sobre o objeto que é certificado;
- Chave de informação pública: que é a chave pública da entidade certificada;
- Assinatura de autoridade em certificação: como o nome já diz, é a assinatura da certificadora, que é necessário para garantir a legitimidade da operação.

4.1.5. Sistemas de Detecção de Intrusão (IDS)

O conceito de detecção de intrusão foi introduzido por Anderson (ANDERSON, 1980), que definiu uma tentativa ou ameaça de intrusão como sendo a possibilidade de ocorrência de uma tentativa deliberada e não autorizada para acessar informações, manipular informações, tornar um sistema não confiável ou indisponível.

Para Amoroso (AMOROSO, 1999), detecção de intrusão é um processo para identificar e responder a atividades maliciosas dirigidas a computadores e recursos de redes. Proctor (PROCTOR, 2001) descreve que detecção de intrusão é a tarefa de coletar informações de uma variedade de fontes e então analisa-las buscando sinais de intrusão e de mau uso.

Para Bace e Mell (BACE e MELL, 2001), sistemas de detecção de intrusão (IDS) são sistemas de softwares ou equipamentos que automatizam o processo de monitoramento de ocorrência de eventos em um sistema de computadores ou redes, procurando por sinais de problemas na segurança. Invasões são causadas por ataques a sistemas através da Internet, usuários internos dos sistemas tentando ganhar acesso onde não foi permitido e usuários autorizados que utilizam os privilégios a eles destinados para usos indevidos.

Um sistema de detecção de intrusão (IDS), que tem como objetivo detectar atividades impróprias, incorretas ou anômalas, é um elemento importante de defesa nas organizações. O IDS pode detectar ataques que são realizados por meio de portas legítimas que são permitidas e que passam pelo firewall. O IDS trabalha como uma câmera ou um alarme contra intrusões, podendo realizar a detecção com base em assinaturas conhecidas ou em desvios de comportamento.

Há vários tipos de IDSs, caracterizados por diferentes propostas de análise e monitoramento. Cada proposta possui uma vantagem sobre a outra, porém todas as propostas podem ser descritas em termos de um modelo genérico de IDS.

Muitos IDSs são formados por três componentes funcionais, que são (BACE e MELL, 2001):

- Fontes de Informações: diferentes informações de eventos determinam se a invasão ocorreu. Estas fontes podem ser tiradas de diferentes níveis do sistema, rede, equipamentos e aplicações de monitoramento mais comuns;

- Análises: a parte do IDS que organiza e dá sentido aos eventos é a fonte de informação, decidindo quando esses eventos indicam que está ocorrendo intrusão ou já aconteceram. As propostas de análise mais comuns são a detecção de abuso e a detecção de anomalias;
- Respostas: a característica das ações do sistema é a detecção de intrusão. Estas ações são agendadas em medidas passivas e ativas. Medidas ativas envolvem intervenções automáticas por parte do sistema. Medidas passivas envolvem relatórios para que administradores de redes tomem as providências necessárias, baseando-se nos relatórios fornecidos.

A arquitetura de um IDS está ligada à forma como seus componentes funcionais encontram-se arranjados em relação uns aos outros. Localização e alvo são alguns fatores que influenciam diretamente na arquitetura do IDS. A estratégia de controle sobre o IDS, que descreve como a entrada e a saída de dados é administrada, são três (BACE e MELL, 2001):

- Centralizada: todo monitoramento, detecção e relatórios são controlados diretamente de uma localização central;

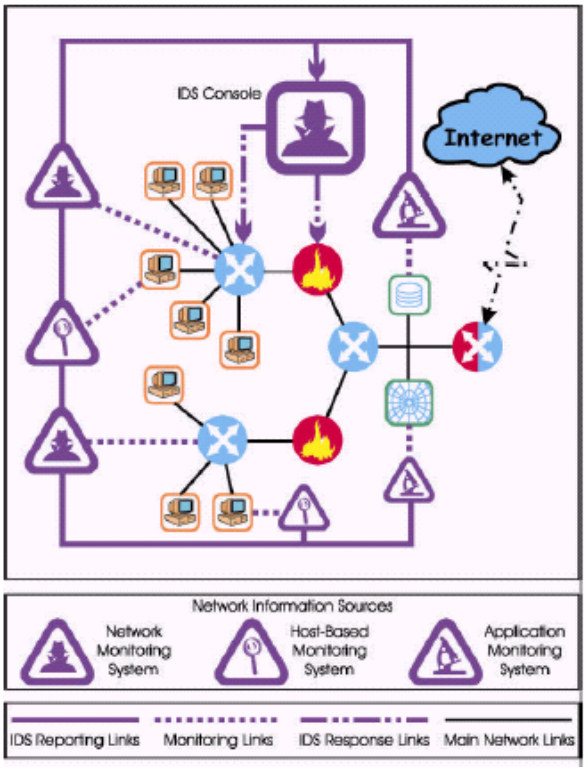

Figura 4.12: Controle de Estratégia Centralizado. Fonte: BACE e MELL, (2001).

- Parcialmente Distribuído: monitoramento e detecção são controlados de um nó de controle central, com relatórios hierárquicos de uma ou mais localizações centrais;

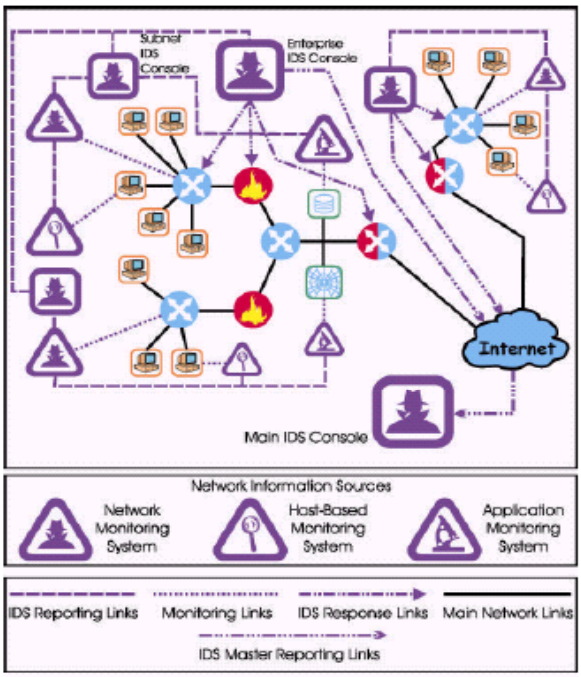

Figura 4.13: Controle de Estratégia de IDS Parcialmente Distribuído. Fonte: BACE e MELL, (2001).

- Totalmente Distribuído: monitoramento e detecção são feitos usando uma aproximação agent-based, onde são tomadas as decisões de resposta no ponto de análise.

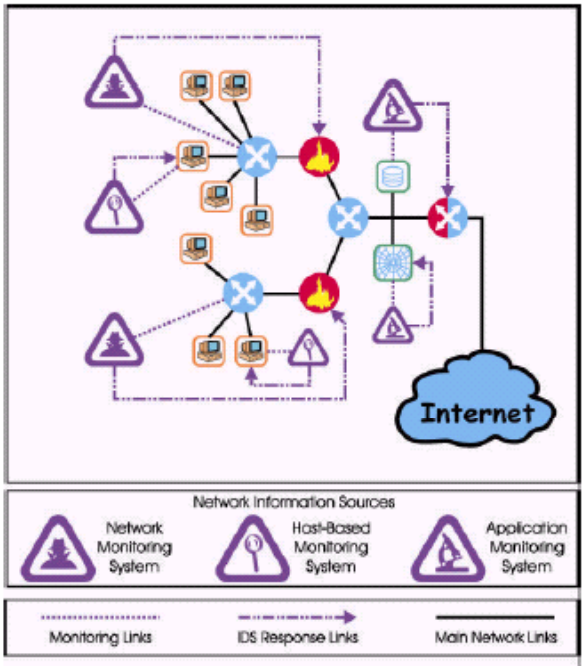

Figura 4.14: Controle de Estratégia de IDS Totalmente Distribuído. Fonte: BACE e MELL, (2001).

O IDS, ao detectar tentativas de ataques externos e internos, dependendo de sua localização, permite que o administrador de segurança tenha conhecimento sobre o que está acontecendo e sobre qual medida tomar com relação ao ataque.

Três tipos de ataques são mais comumente detectados pelo IDS. São eles scanners de sistemas, negação de serviço (DoS) e invasão de sistemas. Estes ataques podem ser lançados localmente ou remotamente através da rede para atingir o alvo. O operador do IDS deve entender a diferença entre cada um destes ataques para poder tomar as devidas respostas.

A dificuldade de detectar se um ataque é realmente um ataque, é o grande desafio dos IDSs. Possuem a função de analisar o tráfego para uma máquina-

destino ou para uma rede-destino, comparando o tráfego com sua base de ataques conhecidos ou no comportamento do tráfego.

A quantidade de tentativas de ataques a organizações são enormes. Segundo o IDGNow, o Brasil ocupou o segundo posto de sites atacados, com 5.586 ataques, perdendo somente para os Estados Unidos com 26.792 sites atacados.

4.1.6. Dados Biométricos

A autenticação tem um papel importante na segurança dos sistemas, ao validar a identificação do usuário e concedendo a autorização de acesso aos recursos computacionais. A autenticação ou validação da identificação do usuário pode ser realizada com base nas características do usuário.

A biometria é um método de autenticação que analisa as características físicas ou comportamentais de um indivíduo, comparando com os dados armazenados no sistema de autenticação (NAKAMURA e GEUS, 2001).

Os dados biométricos estão sendo trabalhados como uma maneira confiável de autenticação. Reconhecer a identidade de uma pessoa através de características fisiológicas como impressões digitais, imagens da retina, identificação de voz, imagens térmicas ou com base em alguma outra característica de seu comportamento como o padrão dos toques de digitação ou escrita manual. (STRAUCH, 2000).

Algumas características físicas utilizadas pela biometria podem ser (NAKAMURA e GEUS, 2001):

- Composição química do odor corporal;
- Características faciais;
- Emissões térmicas;
- Retina;
- Íris do olho;
- Impressões digitais;
- Geometria da mão;
- Poros da pele;
- Análise da assinatura;
- Padrões da escrita;
- Voz.

Dessas características, somente a íris e a impressão digital são consideradas únicas no indivíduo, não existe outra igual.

As tecnologias biométricas mais comuns, utilizadas pelo mercado, são o reconhecimento facial e o reconhecimento de impressões digitais.

Um dos problemas enfrentados pelo sistema de biometria é a sua alta taxa de erro, em função de mudanças de características físicas dos indivíduos com o passar dos anos.

4.2. Algumas Ferramentas de Prevenção

4.2.1. Pretty Good Privacy (PGP)

O PGP é um software de proteção para correio eletrônico e arquivos, que utilizam a criptografia de chaves públicas e privadas de até 1024 bits. Foi desenvolvido por Philip Zimmermam.

A mensagem é criptografada com a chave pública do destinatário e em seguida enviada. Ao chegar no destino, o destinatário possui a chave de codificação e poderá então ler a correspondência. Esta chave de codificação, somente o destinatário final possuí, o que impede que, caso seja interceptada, possa ser lida por outra pessoa (HOLSCHUH, 2000).

Com o PGP é possível fazer as seguintes funções:

- Codificar e decodificar em qualquer aplicação;
- Criar e gerenciar chaves criptográficas;
- Criar arquivos self-decrypting;
- Apagar arquivos e diretórios permanentemente;
- Tráfego seguro na rede.

O PGP é baseado no sistema de encriptação de chave pública, portanto pode gerar pares de chaves consistentes, o que o torna um software de grande aceitação pela comunidade de segurança da informação.

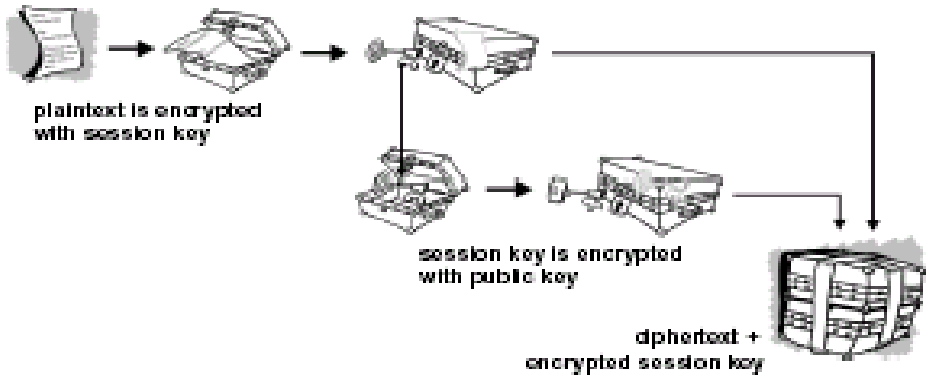

Figura 4.15: Funcionamento da encriptação do PGP. Fonte: Network Associates – An Introdution to Cryptography, (2000).

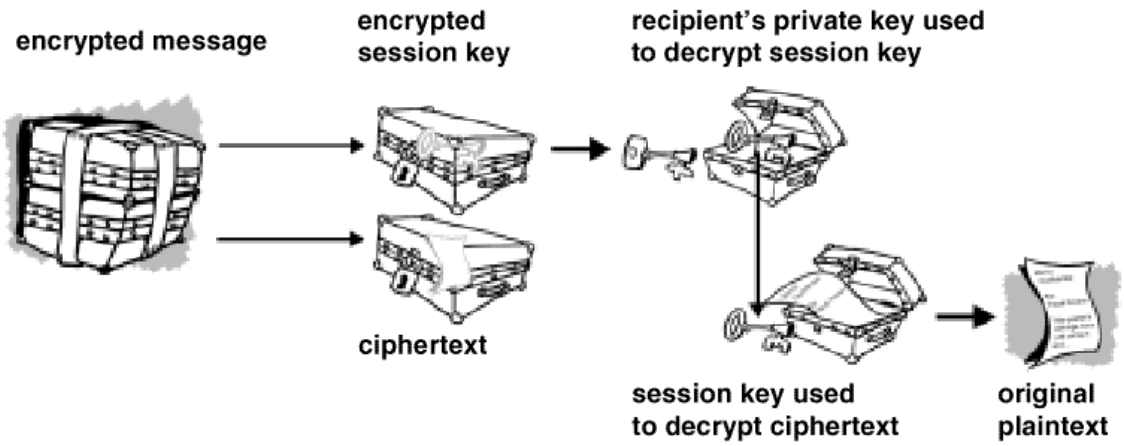

Figura 4.16: Funcionamento da desencriptação dos dados pelo PGP. Fonte: Network Associates – An Introdution to Cryptography, (2000).

4.2.2. Secure Socket Layer (SSL)

O protocolo SSL foi desenvolvido pela Netscape Communications para garantir a segurança de quaisquer dados que estejam trafegando pela internet. Isto somente ocorrerá se o servidor de dados e o cliente possuírem este protocolo.

Uma empresa certificadora fornece um certificado de autenticação para um site na internet permitindo o uso do SSL, fazendo com que o cliente se conecte a internet de modo seguro e possa efetuar a navegação tranqüilamente transparente (OLIVEIRA, 1999).

O SSL é atualmente o mecanismo de segurança mais utilizado na Internet e implementa os seguintes conceitos (FREIER et al, 1996):

- Privacidade dos dados;
- Integridade dos dados;
- Autenticação do servidor;
- Autenticação do cliente (opcionalmente).

4.2.3. Antivírus

Os antivírus são programas específicos, capazes de detectar e eliminar a grande maioria dos vírus de computador, bem como trojans. Este software deve ser constantemente atualizado e sua proteção automática deve ser habilitada. É difícil escolher o antivírus adequado para a organização, porém qualquer um que seja escolhido, é melhor do que não ter nenhum.

Vários autores, dentre os quais cita-se Hagen (HAGEN, 2001), Guttman e Bagwill (GUTTMAN e BAGWILL, 1997) descrevem o modo de operação dos softwares antivírus. Basicamente esses softwares possuem uma base de dados com as assinaturas dos vírus conhecidos. Essas assinaturas são o código dos vírus, que são verificados arquivo por arquivo no processo de busca.

O ponto chave é manter a base de dados atualizada com assinaturas de todos os novos vírus descobertos a cada dia.

O funcionamento dos antivírus é constante, isto é, ficam constantemente monitorando o equipamento para verificar qualquer alteração de funcionamento ou vasculhando os arquivos para verificar se não está infectado.

Todos os usuários de computador, independente de estar em rede, deve ter um programa antivírus em sua máquina e deve saber como funciona e como atualizar. O procedimento de atualização deve ser feito no mínimo mensalmente.

A política de segurança para vírus é classificada por três aspectos, segundo Guttman e Bagwill (GUTTMAN e BAGWILL, 1997):

- Prevenção: tenta evitar a contaminação de qualquer arquivo;
- Detecção: tenta detectar a contaminação de algum arquivo;
- Remoção: tenta remover o vírus do sistema infectado, que pode ser feito através da deleção do arquivo, eliminação do vírus ou, em casos extremos, reinstalação do sistema operacional.

5. PESQUISA NA UNIVERSIDADE ESTADUAL DO OESTE DO PARANÁ - UNIOESTE

5.1. Histórico e Apresentação

Em 1987 surgiu a Universidade Estadual do Oeste do Paraná – UNIOESTE, da fusão e transformação em instituição estadual, com ensino público e gratuito, de quatro faculdades municipais: Fecivel, de Cascavel; Facisa, de Foz do Iguaçu; Facimar, de Marechal Cândido Rondon; e Facitol, de Toledo. Inicialmente como fundação, depois, na condição de autarquia.

O reconhecimento como universidade veio em dezembro de 1994, ano em que foi anunciado o projeto de expansão da sua estrutura física e de cursos. Em 1999, passou a contar com mais um campus, o de Francisco Beltrão, no sudoeste do Paraná. E, mais recentemente, incorporou o Hospital Universitário do Oeste do Paraná.

Possuí 34 cursos de graduação e 23 cursos de Pós-Graduação e um total de 9.335 alunos graduando, 718 alunos de pós-graduação, 940 professores, 985 funcionários.

Em perfeita sintonia com a realidade da região que a acolhe, a UNIOESTE coloca em prática um plano estratégico que atende a necessidade e expectativas da s regiões oeste e sudoeste do Paraná. Alicerçada em proposta multicampi, impõe-se como agente de integração, de difusão do conhecimento e de promoção do desenvolvimento regional.

Com base nessa proposta, orienta suas ações para privilegiar as peculiaridades inerentes à microrregião de cada campus. Nesse sentido, o leque de cursos potencializa a vocação das áreas de saúde e agro-industrialização (Cascavel), de biotecnologia e de alimentos (Toledo), de turismo e de energia elétrica (Foz do Iguaçu) e de agropecuária (Marechal Cândido Rondon). Na mesma direção, o recém-incorporado campus de Francisco Beltrão indica, como setores pontuais, a agricultura baseada em minifúndios e a agroindústria.

5.2. Reitoria da UNIOESTE

A Reitoria da UNIOESTE está localizada na cidade de Cascavel e tem como função principal dar suporte aos demais campus da Universidade. Possuí em sua estrutura 150 estações de trabalho e 11 servidores ligados em rede e todos com acesso à Internet. Sua infra-estrutura de redes é baseada na plataforma Windows. A Diretoria de Informática é o setor responsável por manutenção e desenvolvimento de toda a infra-estrutura de informática da Reitoria bem como de toda a UNIOESTE. Esta diretoria é composta por uma equipe de 22 pessoas distribuídas em desenvolvimento e manutenção de sistemas, desenvolvimento e manutenção de páginas web, manutenção e administração de redes, manutenção e suporte de equipamentos e softwares.

5.3. Política de Segurança da Informação na UNIOESTE – Estudo de Caso

A política de segurança da Universidade é feita por firewalls instalados na Reitoria, e demais campus, sistema de gerenciamento de logs, programas antivírus em estações e servidores, política de acesso lógico.

Para saber o grau de conhecimento e compreensão sobre segurança de informação de alguns funcionários da reitoria, e o nível de risco de segurança, nos meses de maio e junho, foi aplicada uma pesquisa (anexo I), junto a 30 usuários da rede da UNIOESTE-Reitoria, para saber como são tratadas as informações por estes usuários.

5.4. Resultado da Pesquisa

Foram escolhidos 30 usuários da rede UNIOESTE-Reitoria, aleatoriamente, para aplicar os testes. Foram avaliadas informações sobre senha de acesso à rede, manipulação das informações, e situação dos equipamentos.

Deve-se ressaltar, de antemão, que, embora o número de testes seja pequeno (30 respostas), podem-se perceber tendências de comportamento.

No primeiro gráfico, notou-se que na divulgação e manutenção de senhas há uma tendência em manter a senha sigilosa, mas ao criá-la ainda não há uma cultura de utilizar-se de caracteres especiais em sua elaboração.

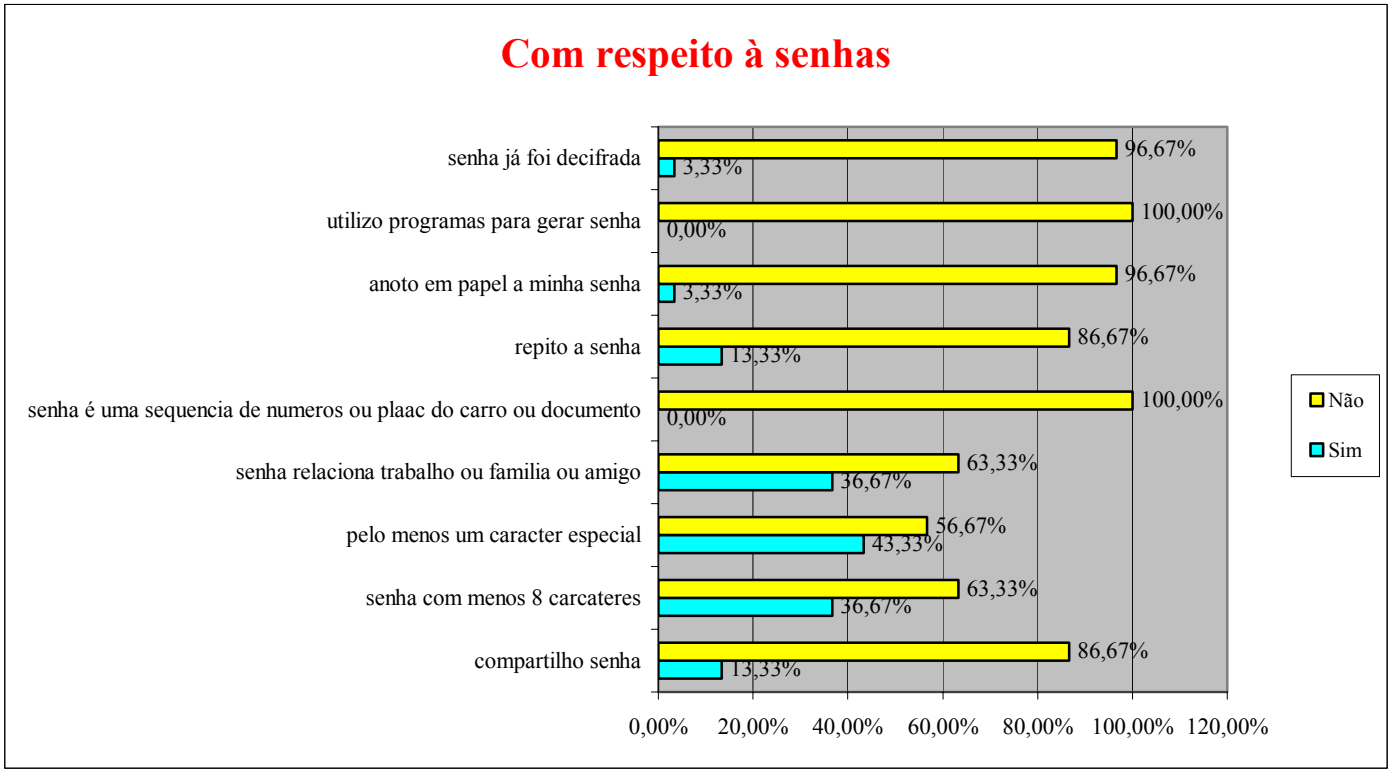

Figura 5.1: Gráfico de respostas à pergunta - Com respeito a senhas?

Quanto à manipulação de informações, as respostas mostram que não existe uma preocupação quanto ao cuidado na manipulação por parte dos usuários. O cuidado ao enviar e receber informações pelo correio eletrônico é descartado por parte do usuário. Já os antivírus instalados, são atualizados, mas não são executados diariamente. A maioria dos entrevistados não guarda cópias das informações trabalhadas em outro equipamento, como o servidor de dados. Estas avaliações podem ser observadas no gráfico seguinte.

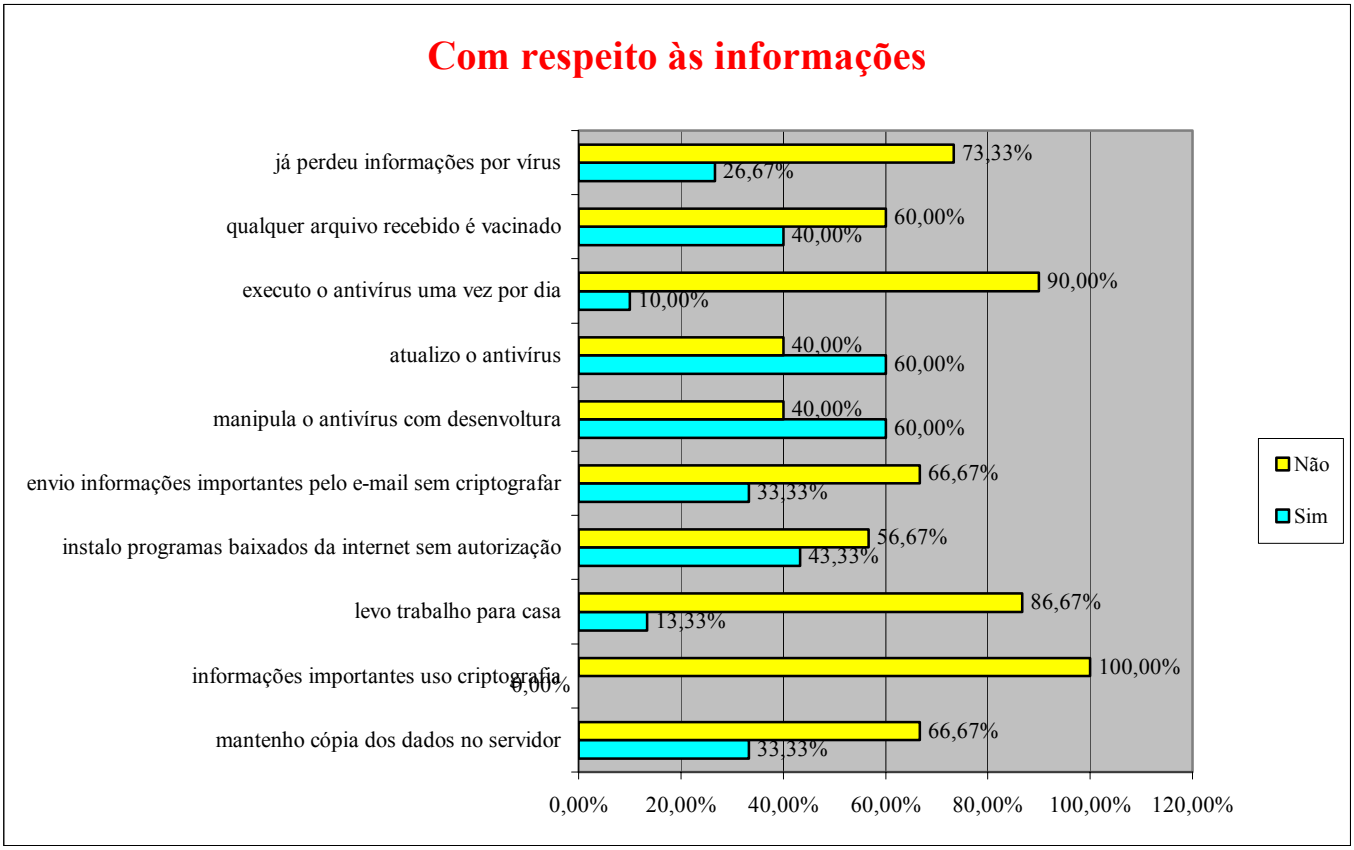

Figura 5.2: Gráfico de respostas à pergunta - Com respeito às informações?

Em relação aos equipamentos, nota-se aqui uma tendência a manter ou seguir as orientações do pessoal técnico de suporte e manutenção. O usuário não movimenta ou instala, na sua maioria, softwares e hardware sem o pessoal técnico fazer por eles. Mesmo assim com relação a software, ainda há uma certa liberdade na utilização destes por parte do usuário.

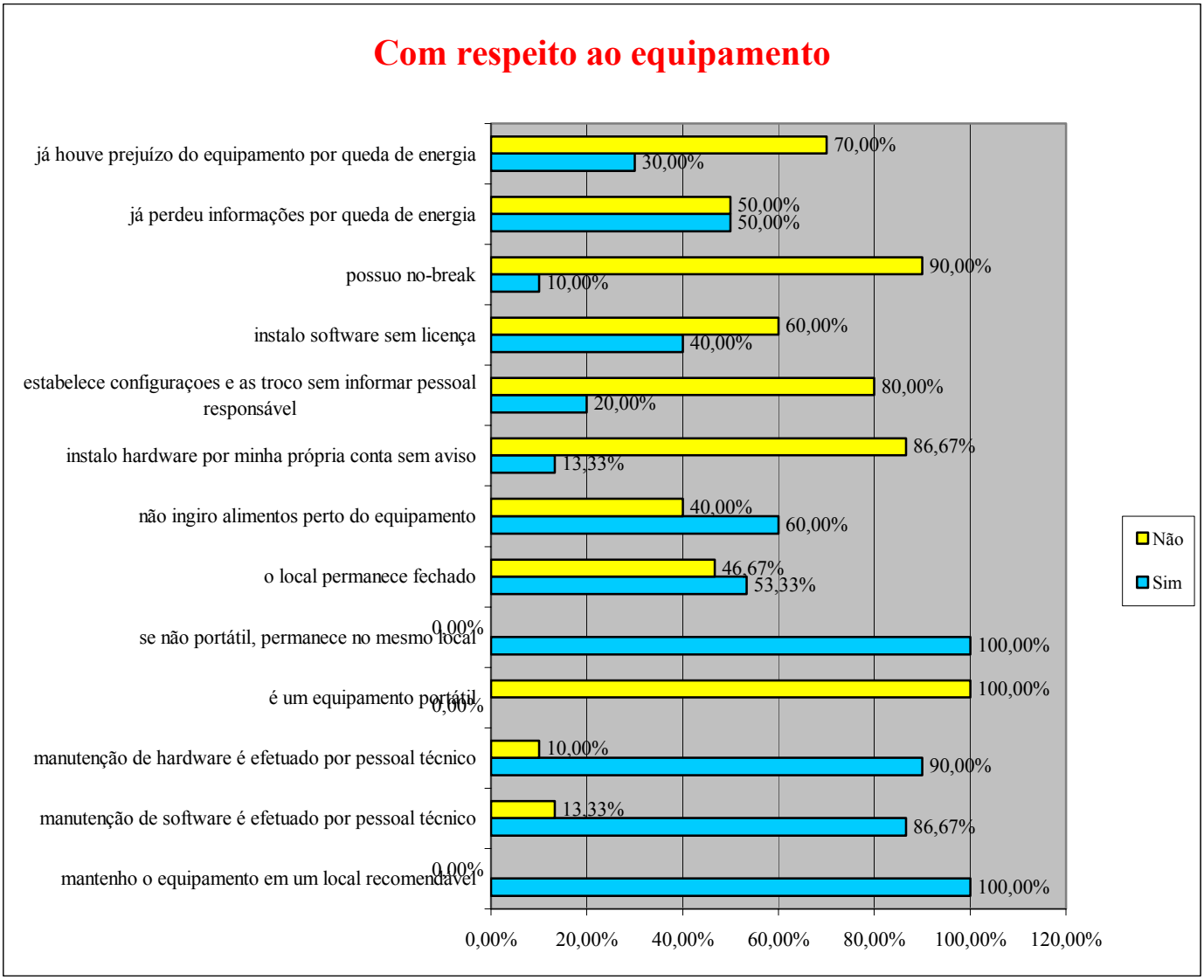

Figura 5.3: Gráfico de respostas à pergunta - Com respeito ao equipamento?

Com base nos gráficos apresentados, observamos a necessidade de educar o usuário quanto à utilização de softwares nos equipamentos, a elaboração e manutenção de senhas, e principalmente, na manipulação das informações trabalhadas.

6. PROPOSTA DE EDUCAÇÃO DE USUÁRIOS DA REITORIA DA UNIVERSIDADE ESTADUAL DO OESTE DO PARANÁ - UNIOESTE

6.1. Proposta de Educação do Usuário

Baseado nos resultados da pesquisa realizada, identificou-se a necessidade de disseminar mais informações relativas à segurança da informação entre usuários de redes de computadores da Reitoria na UNIOESTE.

Esta disseminação da informação seria apresentada através desta Proposta de Educação do Usuário.

A reitoria da universidade é composta de 118 colaboradores diretos e a disponibilidade deste em fazerem cursos durante um período muito longo seria inviável em um primeiro momento. Desta forma vislumbrou-se algumas possibilidades de apresentação e aplicação desta proposta de educação, que seriam o treinamento inicial e emergencial, palestras de curta duração sobre políticas de segurança, uma cartilha com informações de segurança, cursos de atualizações dos colaboradores em períodos mais dispersos.

6.1.1. Treinamento Inicial ou Emergencial

A proposta inicial é elaborar um curso emergencial para usuários disseminadores de informação, entre 30 a 40, que em curso rápidos de 1 ou 2

dias teriam condições de disseminar mais rapidamente alguns conceitos sobre segurança da informação, uma vez que seria impraticável tirar todos os funcionários dos setores.

Tornaria assim um curso emergencial 1 ou 2 usuários de cada setor da reitoria e em ritmo intensivo, fazendo com que estes usuários disseminem estas informações pelos setores de origem. Esta seria uma medida inicial e emergencial.

Esta prática atenderia, num primeiro momento, as necessidades dos usuários mais carentes de informação e a tranqüilidade do administrador de redes de que estaria sendo disseminada a cultura de segurança no ambiente de trabalho.

6.1.2. Palestras Educativas Rápidas

Após a execução do treinamento emergencial, a outra estratégia seria a apresentação de palestras educativas rápidas nos setores sobre elaboração de senhas, a importância de se ter cópias de segurança de dados, a necessidade de atualização de softwares antivírus, esta uma deficiência encontrada durante a realização da pesquisa, onde se observou que a atualização do software era feita somente quando o pessoal de suporte se dirigia até os setores e executava as rotinas de atualização

Esta prática demandaria um tempo um pouco maior para a elaboração de material de divulgação do conteúdo temático das palestras.

Nesta estratégia, a abrangência de pessoas de um mesmo setor seria maior e, após ter sido feita a disseminação inicial por parte do usuário do setor que fez o treinamento emergencial, a palestra teria um maior aproveitamento por parte dos usuários dos setores, reforçando a explanação inicial dos disseminadores dos setores.

6.1.3. Elaboração de Cartilha

Esta proposta seria a elaboração de uma cartilha de segurança e seria uma etapa trabalhada a longo prazo.

Envolveria não somente o pessoal do setor de informática, mas também a estrutura gráfica da universidade, a estrutura pedagógica na elaboração das cartilhas, a equipe de recursos humanos, a qual caberia a função de entregar a cada colaborador um exemplar desta cartilha. O trabalho de elaboração, montagem e divulgação do material, demandaria um período maior de tempo, porém a sua abrangência também seria maior.

Esta cartilha seria elaborada contendo conceitos básicos de segurança, riscos no uso da internet, correio eletrônico, senhas, vírus, engenharia social, vulnerabilidades, programas de troca de arquivos, realização de cópias de segurança (backups), e informações relevantes para o bom uso da informática por parte dos usuários.

6.1.4. Cursos de Periódicos de Atualização

Além das três práticas mencionadas, a realização de cursos periódicos de atualização seria uma necessidade constante dentro da universidade, podendo então ampliar os conhecimentos técnicos dos usuários de informática.

Como a atualização dos softwares utilizados pela universidade se dá constantemente, estes cursos periódicos de atualizações viriam de encontro com as necessidades dos usuários.

Com essas práticas, poderia ser feito um mutirão de conscientização do usuário da necessidade de ter uma política de segurança da informação dentro da universidade e esta política estar atuante e ser respeitada por todos.

Educando o usuário final seria a maneira mais fácil de disseminar esta cultura.

7. CONCLUSÃO

7.1. Algumas Considerações sobre Políticas de Segurança

Muitas vezes, redes corporativas bem estruturadas acabam esbarrando em falhas internas, de usuários não preparados para utilizar os sistemas ali instalados. Um bom começo de estruturação de uma política de segurança é a conscientização dos usuários por parte do pessoal responsável pela segurança de dados. Educar o usuário é a melhor política de segurança que pode ser aplicada na organização.

A segurança não é estática, deve ser revista constantemente. Deve se ter na equipe, pessoas em constante vigília e informados de falhas/bugs de sistemas operacionais, gerenciadores de banco de dados, falhas em programas em geral. Analisar o acesso interno e externo para não ter surpresas.

Algumas recomendações são colocadas a seguir, não como uma solução final, mas como uma ajuda à implementação de uma política de segurança.

Política de Segurança é a linha de frente de defesa contra qualquer ataque, é um documento muito importante na organização e deve ser conhecido por todos os funcionários. Este documento define o que deve se fazer quando há uma quebra de segurança, removendo o mistério e o pânico causado durante e/ou após uma invasão. A política deve definir quais sistemas são críticos, o que precisa de proteção e como será protegido. Quem deve proteger e se

responsabilizar, quem é o grupo de segurança ou o Computer Emergency Response Team –CERT.

O documento que define a política de segurança deve ser de fácil compreensão para qualquer um que o leia. Um dos aspectos importantes da política é determinar o que é importante e quanto importante é este sistema ou serviço, e como proteger. Segundo a Internet Security Alliance (ISA, 2002), "Identificar os impactos adversos, incluindo os financeiros, reputação, posicionamento no mercado, produtividade/tempo. Quantificar os impactos financeiros o mais extensível possível".

No ano de 2002, segundo a Symantec (SYMANTEC, 2003), os ataques diminuíram, porém os estragos a cada ataque foram maiores. O número de vulnerabilidades aumentou em 81% em relação a 2001.

Ainda, segundo a pesquisa da Symantec, 29,5% dos ataques no segundo semestre e 2002 foram diretamente sobre o gerenciador de banco de dados Microsoft SQL, o qual indica que, quando instalado com as configurações default ele é potencialmente vulnerável. Verificações devem ser feitas para garantir que o servidor está com as correções necessárias e o hardware está protegido. Na tabela abaixo são exibidos outros tipos de falhas encontradas em diversos softwares e protocolos.

Top 20 Scans
(July 1, 2002 – Dec 31, 2002)

Scan Type	Percent of Total Scans
Microsoft SQL Server	29.5%
HTTP	16.5%
FTP	13.3%
Netbios Name Service	13.0%
HTTPS	4.0%
SSH	3.2%
SMTP	3.1%
RPC (tcp)	2.5%
SubSeven	2.0%
Netbios (139/tcp)	1.8%
Netbios (445/tcp)	1.7%
SOCKS (1080/tcp)	1.3%
CDE Subprocess Control	1.1%
57/tcp	1.0%
Telnet	0.9%
Squid Proxy	0.9%
LPD	0.8%
135/tcp	0.6%
DNS	0.6%
1524/tcp (Ingreslock)	0.4%

Figura 6.1: Falhas encontradas pela Symantec no segundo semestre de 2002. Fonte: Symantec Internet Security Threat Report (2003).

A melhor maneira de se proteger dos hackers é se proteger das vulnerabilidades mais comuns. A melhor segurança é garantir que as instalações do sistema operacional na seja a instalação default e as atualizações estejam sendo feitas conforme o fabricante recomenda.

Outro ponto é, porque ter portas de firewall abertas se não serão usadas. Firewalls são a principal defesa de perímetro, guardando o gateway para impedir invasões. É uma ferramenta muito útil.

Não importa quantos equipamentos estão distribuídos através da rede, nunca haverá segurança suficiente para garantir que está 100% seguro. Uma combinação entre tecnologia, conhecimento e educação irá prover camadas de

segurança e garantirá mais proteção. A única maneira de proteger-se contra a internet é não estar conectado a ela.

Basear a política de segurança em fatos e conhecimento, garantir as correções em estratégias e ser realista com suas condições é o melhor meio de elaborar sua política.

Sem dúvida, a tecnologia é peça fundamental em uma estratégia, mas não há política de segurança que se sustente sem dois pilares distintos: processos e pessoas. Por trás de uma política existe uma pessoa, e o que define o sucesso da iniciativa é a sua consciência. A falta de padrões e treinamento é um dos maiores obstáculos para se implantar uma política de segurança.

7.2. Conclusões

Neste trabalho foram descritos alguns mecanismos de ataques a computadores em rede, alguns perigos em potencial e algumas ferramentas de prevenção a estes ataques.

No estudo de caso junto à Universidade Estadual do Oeste do Paraná – UNIOESTE, ficou evidente que, além da utilização de ferramentas tecnológicas, a educação dos usuários é um fator preponderante na elaboração de uma política de segurança.

Observou-se que usuários despreparados e mal informados executam tarefas mecanicamente e não existe a preocupação quanto ao destino dado as informações manuseadas. Além de ter verificado que em sua maioria os usuários

da rede UNIOESTE-Reitoria não fazem cópias de segurança de seus dados, não conhecem técnicas como criptografia de dados, programas geradores de senha, verificou-se a necessidade de investimentos em treinamento do usuário da rede.

Na proposta para conscientizar e educar os usuários pode ser verificado métodos simples de aprendizagem, como a elaboração de uma cartilha que pode conter algumas regras básicas de segurança e manipulação de informações, porém este método inicial abre caminho para a melhor aceitação de uma política de segurança a ser implementada no decorrer do processo de conscientização e educação dos usuários.

O ativo humano oferece um dos maiores índices de riscos. Diante dessa percepção, confirmada pelas últimas pesquisas de segurança, as organizações devem investir maciçamente na conscientização dos funcionários, na capacitação dos operadores de processos críticos e principalmente dos usuários finais, que detém uma parcela representativa de responsabilidade quando manuseiam, armazenam, transportam e descartam informações.

O maior desafio de uma política de segurança não é inicia-la, e sim sustenta-la na organização, verificando permanentemente se as normas estão sendo cumpridas e se há necessidade de atualizações. Para evitar que a política termine em um amontoado de papéis esquecidos em alguma gaveta, a iniciativa deve ser disseminada maciçamente entre todos os funcionários. O setor de recursos humanos da organização deve estar atuante nesta disseminação. Com uma estratégia permanente de conscientização, a obrigação torna-se hábito.

O objetivo de uma política de segurança é minimizar riscos. Deve se levar em conta a relação custo/benefício na hora de implementar uma política de segurança.

Para que uma política de segurança se torne efetiva, ela deve ter a aceitação e o suporte de todos os níveis de empregados da organização. O principal propósito da política de segurança é informar aos usuários e equipes, as suas obrigações para a proteção da tecnologia e do acesso da informação (RFC-2196).

As características de uma boa política de segurança são:

- Deve ser implementável através de procedimentos de administração, publicação das regras de uso aceitáveis, ou outros métodos apropriados;
- Deve ser exigida com ferramentas de segurança onde apropriado, e com sanções onde a prevenção efetiva não seja tecnicamente possível;
- Deve definir claramente as áreas de responsabilidade para os usuários, administradores e gerentes.

Uma vez que a política tenha sido estabelecida, deve ser claramente comunicada aos funcionários da organização. Uma parte importante do processo é a criação de um documento em que os usuários assinem, dizendo que leram, entenderam e concordaram com a política estabelecida. Um exemplo deste documento está no anexo II deste trabalho.

7.3. Perspectivas para Trabalhos Futuros

Uma possível proposta de trabalho futuro poderia ser uma análise mais detalhada sobre como estão sendo administradas as ferramentas de proteção em uso pela universidade, como firewall, e IDS, por exemplo.

Acompanhar o processo de educar o usuário através de métodos de educação a distância, tão utilizados atualmente.

8. ANEXOS

8.1. Anexo I

Teste de Segurança para Usuários da Rede UNIOESTE/REITORIA

Instruções:

- Responda SIM ou NÃO para as seguintes questões;
- Se a questão não se aplica ao seu equipamento deixe sem resposta.

1) COM RESPEITO À SUA SENHA.
    a. Compartilho a minha senha de acesso ao servidor com meus companheiros de trabalho?
    b. Minha senha tem menos de 8 caracteres?
    c. Minha senha tem pelo menos um caracter especial, como estes (!”$%&/=?;)?
    d. Minha senha tem a ver com algo de meu lugar de trabalho, minha família ou amigo?
    e. Minha senha tem a ver com uma seqüência de números, placa de meu carro ou identificação de algum documento?
    f. Costumo repetir minha senha para não esquecê-la?
    g. Para que não me esqueça da senha anoto em um local seguro, mas dentro do meu local de trabalho?
    h. Costumo utilizar programas que geram a senha para mim?
    i. Minha senha já foi decifrada uma vez?

2) COM RESPEITO AO MANEJO DAS INFORMAÇÕES
    a. Mantenho uma cópia atualizada das informações no servidor?
    b. As informações importantes da empresa, manuseio-as com criptografia?
    c. Levo trabalho da empresa para fazer em casa?
    d. Instalo programas que baixo da internet, sem autorização do administrador de redes, que me facilitam um pouco o trabalho?
    e. Envio informações importantes por correio eletrônico (e-mail), sem encriptá-las?
    f. Sei manejar completamente o antivírus que está instalado em meu equipamento?
    g. Atualizo regularmente (uma vez ao mês) o antivírus?

h. Executo o antivírus pelo menos uma vez ao dia?
i. Qualquer arquivo que chega para meu equipamento, seja uma página web, correio eletrônico (e-mail), ftp de arquivos ou disquete, é vacinada?
j. Já perdi informações por causa de vírus?

3) COM RESPEITO AO EQUIPAMENTO
   a. Mantenho o equipamento em um local recomendável (se portátil)?
   b. Manutenção de software é efetuado por pessoal técnico especializado?
   c. Manutenção de hardware é feito por pessoal técnico especializado?
   d. É um equipamento portátil?
   e. No caso de não ser portátil, permanece no mesmo local sempre?
   f. O local permanece fechado?
   g. Evito ingerir alimentos perto do equipamento?
   h. Instalo hardware por minha própria conta e não aviso o pessoal encarregado por este procedimento?
   i. Estabelece configurações e as troca sem informar o pessoal encarregado por este procedimento?
   j. Instalo programas sem providenciar a licença do software com o pessoal encarregado por este procedimento?
   k. Possuo algum equipamento de no-break em meu equipamento para garantir a falta de luz?
   l. Já perdi informações importantes por causa de quedas de energia abruptamente?
   m. Já houve algum prejuízo ao equipamento por queda de energia abruptamente?

4) COMENTÁRIOS E OBSERVAÇÕES

8.2. Anexo II

Documento de Conhecimento da Política de Segurança

Declaração de Aceite para Normas de Uso de Sistemas Computacionais

Acceptable Use Statement for [COMPANY NAME] Computing Systems

The following document outlines guidelines for use of the computing systems and facilities located at or operated by ([COMPANY NAME]).

The definition of [COMPANY NAME] Computing Systems will include any computer, server or network provided or supported by [COMPANY NAME] Computing Systems.

Use of the computer facilities includes the use of data and/or programs stored on [COMPANY NAME] Computing Systems, data and/or programs stored on magnetic tape, floppy disk, CD ROM, or any storage media that is owned and maintained by [COMPANY NAME] Computing Systems.

The "user" of the computing system is the person requesting an account (or accounts) in order to perform work in support of a [COMPANY NAME] program or a project authorized for the [COMPANY NAME] Systems Division. The purpose of these guidelines is to ensure that all [COMPANY NAME] users (business users, support personnel, technical users, and management) use the [COMPANY NAME] Systems Division computing facilities in an effective, efficient, ethical and lawful manner.

[COMPANY NAME] accounts are to be used only for the purpose for which they are authorized and are not to be used for non [COMPANY NAME] related activities.

Unauthorized use of a [COMPANY NAME] account/system is in violation of Section 799, Title 18, U.S. Code, and constitutes theft and is punishable by law.

Therefore, unauthorized use of [COMPANY NAME] Systems Division computing systems and facilities may constitute grounds for either civil or criminal prosecution.

In the text below, "users" refers to users of the [COMPANY NAME] Systems Division computing systems and facilities.

The [COMPANY NAME] Systems Division computing systems are unclassified systems. Therefore, classified information may not be processed, entered or stored on a [COMPANY NAME] Systems Division computing system. Information is considered

"classified" if it is Top Secret, Secret and/or Confidential information which requires safeguarding in the interest of National Security.

Users are responsible for protecting any information used and/or stored on and/or in their [COMPANY NAME] accounts. Consult the [COMPANY NAME] User Guide for guidelines on protecting your account and information using the standard system protection mechanisms.

Users are requested to report any weaknesses in [COMPANY NAME] computer security, any incidents of possible misuse, or any violation of this agreement to the proper authorities by contacting [COMPANY NAME] User Services or by sending electronic mail to security@companyname.com.

Users shall not attempt to access any data, projects and/or programs contained on [COMPANY NAME] systems for which they do not have authorization or explicit consent of the owner of the data, project and/or program, the [COMPANY NAME] Division Chief or the [COMPANY NAME] Data Processing Installation Computer Security Officer (DPI-CSO).

Users shall not divulge Dialup or Dialback modem phone numbers to anyone.

Users shall not share their [COMPANY NAME] account(s) with anyone. This includes sharing the password to the account, providing access via an .rhost entry or other means of sharing.

Users shall not make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.

Users shall not make copies of system configuration files (e.g. /etc/passwd) for their own, unauthorized personal use or to provide to other people and/or users for unauthorized uses.

Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of systems; deprive an authorized [COMPANY NAME] user access to a [COMPANY NAME] resource; obtain extra resources, beyond those allocated; circumvent [COMPANY NAME] computer security measures or gain access to a [COMPANY NAME] system for which proper authorization has not been given.

Electronic communication facilities (such as Email or Newsgroups) are for authorized [COMPANY NAME] use only. Fraudulent, harassing or obscene messages and/or materials shall not be sent from, to or stored on [COMPANY NAME] systems.

Users shall not download, install or run security programs or utilities that could potentially reveal weaknesses in the security of a system. For example, [COMPANY NAME] users shall not run password cracking, key logging, or any other potentially malicious programs on [COMPANY NAME] Systems Division computing systems.

Any noncompliance with these requirements will constitute a security violation and will be reported to the management of the [COMPANY NAME] user and the [COMPANY NAME] DPI-CSO and will result in short-term or permanent loss of access to [COMPANY NAME] Systems Division computing systems. Serious violations may result in civil or criminal prosecution.

I have read and understand the [COMPANY NAME] Systems Division computing systems Use Ethics Statement for use of the [COMPANY NAME] computing facility and agree to abide by it.

Signature: Date:

9. REFERÊNCIAS

ALLEN, Julia H.. **The CERT Guide to System and Network Security Practices**. First printing, Boston-MA-EUA, Addison-Wesley, 2001.

AMOROSO, Edward. **Intrusion Detection:** An Introduction to Internet Surveillance, Correlation, Trace Back, Traps and Response. Sparta-NJ-EUA, Intrusion.Net Books, 1999.

ANDERSON, James P.. **Computer Security Threat Monitoring and Surveillance.** Fort Washington, James P. Anderson Co., 1980.

ANÔNIMO. **Segurança Máxima: O Guia de um Hacker para proteger seu site na Internet e sua rede**. Rio de Janeiro, Campus, 2000.

BACE, Rebecca, MELL, Peter. **Intrusion Detection Systems:** NIST Special Publication on Intrusion Detection System – DRAFT sp800-31. disponível em <http://www.nist.gov>,2001.

BARBOSA, Alexandre. **E-Business com segurança, Internet Business**. São Paulo, ano 5, nº 49, p. 27, set. 2001.

BERNSTEIN, Terry, BHIMANI, Anish B., SCHULTZ, Eugene, SIEGEL, Carol A. . **Segurança na Internet**. Rio de Janeiro, Campus, 1997.

CAIS-RNP. **Relatório Anual 2002.** Disponível em <http://www.rnp.br>. Acesso em: 10 de março de 2003

CERT-CC. **Estatísticas 1988-2001 – Carnegie Mellon University.** Disponível em <http://www.cert.org>. Acesso em: 30 de novembro de 2001

CERT-CC. **Estatísticas 1988-2002 – Carnegie Mellon University.** Disponível em <http://www.cert.org>. Acesso em: 20 de fevereiro de 2003

CERT-RS. **Identificando Recursos.** Disponível em <http://www.cert-rs.tche.br/docs.html/segheck.html>. Acesso em: 22 de novembro de 2001

CSI/FBI–2002. **Computer Crime and Security Survey.** Disponível em <http://www.gocsi.com>. Acesso em: 20 de novembro de 2002.

CSI/FBI–2003. **Computer Crime and Security Survey.** Disponível em <http://www.gocsi.com>. Acesso em: 20 de junho de 2003.

DIJKER, Barbara L. . **A Guide to Developing Computing Policy Documents**. The USENIX Association, 1st edition, setembro, 1996.

DONADO, Siler Amador; ZAMBRANO, Miguel Angel N., FLECHAS, Andrés. **Seguridad Computacional: Libro de Consulta para Administradores y Usuarios.** Universidad del Cauca, Colômbia, Facultad de Ingeniería Electrónica y Telcomunicaciones. 2001.

FREIER, Alan O., KARLTON Philip, KOCHER, Paulo C.. **The SSL Protocol - Version 3.0.** Netscape Corp., november, 1996.

GUTTMAN, Barbara, BAGWILL, Robert. **DRAFT – Internet Security Policy: A Technical Guide.** NIST Special Publication 800-xx, 1997.

HAGEN, Richard D.. **A User's Guide to Security Threats on the Desktop.** Disponível em <http:// sans.org >. Acesso em 04 de maio de 2002.

INFO Exame. **Soluções para a era de Internet.** Ano 15. nº. 173, p 58, agosto 2000.

INFORMÁTICA. **Hacker: Anjo ou Demônio.** Ano 1, nº 3, p 26 - 33, março 2002.

JASONBS. **Política de Segurança da Informação.** Disponível em <http://geocities.yahoo.com.br/jasonbs_1917/seguranca/politica.htm>. Acesso em 04 de maio de 2002.

MADRIGAL, Daniel Ramón Elorreaga. **Firewalls e Seguridad em Internet**. Disponível em: <http://intranet.frsfco.utn.edu.ar/redesdeinfo/seguridad/default.htm>. Acesso em: 26 de março de 2003.

MAIA, Luiz Paulo. **Criptografia e Certificado Digital**. Disponível em: <http://www.training.com.br/pub_seg_cripto.htm>. Acesso em: 26 de novembro de 2001.

MARQUES, Alexandre Fernandez. **Segurança em Redes IP**. Disponível em: <http://www.modulo.com.br/pdf/trab_alexandre_fernandez.pdf>. Acesso em: 26 de novembro de 2001.

McCLURE, Stuart. ; SCAMBRAY, Joel ; KURTZ, George. **Hackers Expostos: Segredos e Soluções para a Segurança de Redes**. 1ª edição, São Paulo, Makron Books, 2000.

MODULO SECURITY SOLUTIONS. **Orçamento Dedicado à Segurança será maior em 2002.** Disponível em <http://www.modulo.com.br>. Acesso em: 22 de novembro de 2001

MODULO SECURITY SOLUTIONS. **7ª Pesquisa Nacional Sobre Segurança da Informação.** Disponível em <http://www.modulo.com.br>. Acesso em: 20 de agosto de 2001

MODULO SECURITY SOLUTIONS. 8ª **Pesquisa Nacional Sobre Segurança da Informação.** Disponível em <http://www.modulo.com.br>. Acesso em: 20 de novembro de 2002

MOREIRA, Stringasci Nilton. **Segurança Mínima: uma visão coorporativa da segurança de informações.** Rio de Janeiro, Axcel Books, 2001.

NAKAMURA, Emílio Tissato; GEUS, Paulo Lício de. **Segurança de Redes: em ambientes cooperativos.** São Paulo, Editora Berkeley, 2002.

NBSO–2003. **Estatísticas de Incidentes Reportados.** Disponível em <http://www.nbso.nic.br>. Acesso em: 05 de julho de 2003.

OLIVEIRA, Wilson José. **Hacker Invasão e Proteção.** Florianópolis, Visual Books, 1999.

PROCTOR, Paul. **Pratical Intrusion Detection Handbook**. Upper saddle River-NJ-EUA, Prentice Hall, 2001.

RAYMOND, Eric S.. **A Brief History of Hackerdom.** Disponível em < http://catb.org/~esr/writings/hacker-history/hacker-history.html >. Acesso em: 30 de março de 2002.

RFC-2828. **Request for Coment: Internet Security Glossary.** Disponível em < http://www.ietf.org/rfc/rfc2828.txt>. Acesso em: 20 de fevereiro de 2002.

SCHNEIER, Bruce. **Security Pitfalls in Cryptography.** Couterpane Systems, 1998. Disponível em <http://www.itsecurity/papers/99.htm>. Acesso em 20 de agosto de 2002.

SYMANTEC. **Symantec Internet Security Threat Report.** Disponível em <http://www.symantec.com>. Acesso em: 20 de abril de 2003

TANENBAUM, Andrew S.. **Redes de Computadores.** Rio de Janeiro, Campus, 1994.

TRINTA, Fernando A. Mota; MACÊDO, Rodrigo C. **Um Estudo sobre Criptografia e Assinatura Digital**. Disponível em: <http://www.ufpe.br>. Acesso em: 30 de outubro de 2002.

WADLOW, Thomas. **Segurança de Redes** 1ª edição, Rio de Janeiro, Campus, 2000.

ZWICKY, Elizabeth D., COOPER, Simon, CHAPMAN, D. Brent. **Construindo Firewalls para a Internet**. Tradução da 2ª edição, Rio de Janeiro, Campus, 2000.